

Telefónica

Informe de **Transparencia** en las Comunicaciones **2019**

ÍNDICE


Reino Unido
Alemania
España


Mexico
Venezuela
Colombia
Ecuador
Perú
Brasil
Chile
Uruguay
Argentina

Introducción y alcance del Informe

En nuestro compromiso con los derechos fundamentales de privacidad y libertad de expresión, publicamos el quinto Informe de Transparencia de las telecomunicaciones, con el objetivo de contribuir a generar una sociedad más abierta y transparente.

El respeto y la promoción de los derechos humanos y, en particular la privacidad y la libertad de expresión, adquieren en el mundo digital una nueva dimensión gracias al uso de las nuevas tecnologías, la Inteligencia Artificial y el protagonismo de los datos a escala global.

Tal y como ocurre en otras empresas de nuestro sector, en Telefónica recibimos solicitudes (ver definición en glosario) de información referidas a las comunicaciones de nuestros clientes o usuarios, solicitudes de bloqueo de acceso a ciertos sitios o contenidos o de filtrado de contenidos, o solicitudes con el objetivo de suspender temporalmente el servicio en determinadas zonas o determinadas cuentas. Dichas solicitudes están cursadas por los cuerpos y fuerzas de seguridad del Estado, organismos gubernamentales y/o juzgados, (en adelante: Autoridades Competentes, ver definición en glosario).

Por ello, la transparencia es un ejercicio imprescindible en un mundo en el que se comparten espacios de responsabilidad a la hora de preservar y garantizar los derechos de las personas.

En este ejercicio de transparencia, nuestro informe muestra:

i. nuestra gobernanza en derechos humanos y específicamente en la privacidad y libertad de expresión;

ii. nuestra debida diligencia en los derechos humanos;

iii. los compromisos, políticas y procesos que seguimos cuando respondemos a las solicitudes de las Autoridades Competentes;

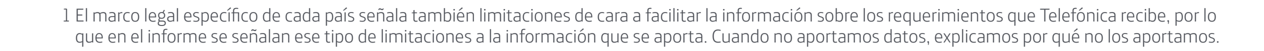
iv. la información sobre el contexto legal que da potestad legal a las autoridades para hacer este tipo de solicitudes[1];

v. las autoridades que tienen potestad según la legislación local para cada uno de los indicadores que reportamos;



vi. el número total de solicitudes que recibimos durante el último año en cada uno de nuestros países de operación, a menos que se nos prohíba hacerlo o a menos que un gobierno u otra entidad pública ya revele dicha información;

vii. y además, y cuando técnicamente es posible, reportamos el número de solicitudes que rechazamos, los accesos que son afectados por cada indicador y las url´s y/o IPs afectadas en el caso de bloqueo y restricción de contenidos.


1 El marco legal específico de cada país señala también limitaciones de cara a facilitar la información sobre los requerimientos que Telefónica recibe, por lo que en el informe se señalan ese tipo de limitaciones a la información que se aporta. Cuando no aportamos datos, explicamos por qué no los aportamos.

Nuestra gobernanza

Tenemos establecido un modelo de gestión de responsabilidades claras en la protección de los derechos humanos en general y en privacidad y libertad de expresión en particular.

Nuestras actividades en materia de derechos humanos se definen e implementan a través del Plan de Negocio Responsable, que establece la estrategia y los objetivos de sostenibilidad de la empresa, y que es aprobado y supervisado por el Consejo de Administración y el Comité de Sostenibilidad y Calidad (uno de los comités permanentes).

Nuestra Política de Derechos y Humanos y nuestra debida diligencia que se basan, entre otras cosas, en los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas y los principios de la Global Network Initiative (GNI), forman parte integral del Plan de Negocio Responsable.

Este modelo de gobernanza, encabezado por el Consejo de Administración y la Oficina de Negocio Responsable en la que participan todos los departamentos pertinentes, tiene como objetivo garantizar que nuestro compromiso con los derechos humanos se incorpore a todas las actividades y niveles de la empresa.

CONSEJO DE ADMINISTRACIÓN
Aprueba el Plan de Negocio Responsable (que incluye objetivos/medidas en relación con los derechos humanos/ privacidad/ libertad de expresión).

SECRETARIO DEL CONSEJO Y ASUNTOS REGULATORIOS
Forma parte del Consejo de Administración y es responsable, entre otras cosas, de promover la privacidad/ libertad de expresión con los grupos de interés externos relevantes en la materia.

COMISIÓN DE SOSTENIBILIDAD Y CALIDAD (Comisión permanente del Consejo)
Supervisa la implementacion del Plan de Negocio Responsable (que incluye objectivos/medidas en relacion con derechos humanos/privacidad/libertad de expresion) a traves de un reporte mensual.

COMISIÓN DE AUDITORÍA Y CONTROL (Comisión permanente del Consejo)
Supervisa, entre otras cosas, cuestiones específicas relacionadas con la privacidad y la libertad de expresión mediante la presentación periódica de informes por parte del *Compliance Officer* y el *Data Protection Officer.*

OFICINA DE NEGOCIO RESPONSABLE
La Oficina de Negocio Responsable (liderada por la Dirección de Ética Corporativa y Sostenibilidad) reúne a todos los directores de departamento relevantes en la Compañía para definir y monitorear el Plan de Negocio Responsable.

COMPLIANCE/DATA PROTECTION OFFICER
Es la función responsable dentro del Grupo de las cuestiones de privacidad.






Asimismo, el *Data Protection Officer* (DPO) es el responsable dentro del Grupo de la protección de datos personales y reporta directamente al Consejo de Administración a través de la Comisión de Auditoría y Control (Comisión permanente del Consejo). El DPO coordina el *Steering Committee* en el que participan todas las áreas corporativas relevantes para asuntos específicos relacionados con la privacidad y la libertad de expresión. Como miembro de la Oficina de Negocio Responsable, el DPO también reporta regularmente a dicha Oficina las cuestiones relacionadas con su función.

Además, el Secretario General y Asuntos Regulatorios forma parte del Consejo de Administración y es responsable, entre otras cosas, de promover la privacidad y la libertad de expresión con los grupos de interés externos relevantes en la materia. En esta función, también dirigió la publicación y difusión del 'Manifiesto Digital' en 2018, en el que se aboga por la cooperación entre los gobiernos, las empresas y la sociedad civil para definir un *New Digital Deal*' que adapte el entorno normativo actual a la era digital, prestando especial atención a las cuestiones de la privacidad y la libertad de expresión.

Para los asuntos de Privacidad y Libertad de Expresión relacionados con los requerimientos de las autoridades contamos con el Comité de Transparencia integrado por los responsables de las áreas globales de Secretaría General, Cumplimiento, Auditoría Interna y Ética Corporativa y Sostenibilidad, quienes analizan los datos reportados de este informe, y pueden realizar las observaciones que consideren pertinentes, con carácter general o específicamente en relación con la información facilitada por las operadoras, con el objetivo de asegurar en todo momento la calidad de la información, como evidencia del cumplimiento de la normativa vigente y de la protección de los derechos fundamentales de las personas.

Aquellas solicitudes que por sus características y excepcionalidad así lo requieren, son analizadas por los máximos responsables de cada área responsable, mediante la adecuada ponderación de todos los intereses potencialmente comprometidos, incluidos los derechos humanos, libertades fundamentales u otros intereses que pudieran ser de aplicación y, si se diesen las circunstancias, por los órganos que dentro de cada compañía tengan entre sus funciones la evaluación y gestión de situaciones que pudieran eventualmente desembocar en una crisis.

En caso de crisis, se sigue un procedimiento establecido en el Sistema Global de Gestión de Crisis, en cuya taxonomía de incidentes críticos que pueden dar lugar a una crisis se enumeran las solicitudes de las autoridades que tienen un impacto en la libertad de expresión y la privacidad, así como "legislaciones con un posible alto impacto negativo en los derechos humanos (libertad de expresión, etc.)". El Sistema Global de Gestión de Crisis prevé que, en caso de una crisis relacionada con la cuestiones de libertad de expresión, el Presidente del Comité de Crisis puede convocar la denominada "Mesa Redonda de Derechos Humanos" (integrada por



los departamentos pertinentes) para analizar la situación y diseñar y aplicar una estrategia de respuesta, informar al Comité Ejecutivo y realizar un análisis posterior con el fin de evitar un riesgo en el futuro.



Nuestra debida diligencia en derechos humanos

Desde 2006 los derechos humanos forman parte integral de nuestros Principios de Negocio Responsable. Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas nos han servido de guía fundamental para fomentar la garantía y respeto del derecho de las personas y, específicamente, en lo referente a la privacidad y libertad de expresión.

De acuerdo con nuestra Política Global de Derechos Humanos contamos con una debida diligencia para identificar, prevenir, mitigar y remediar los impactos (potenciales y reales) en los derechos humanos. Una parte integral de nuestra debida diligencia son las evaluaciones de impacto, que se llevan a cabo cada cuatro/cinco años a nivel global con la ayuda de expertos externos en derechos humanos y en estrecha consulta con nuestros grupos de interés. El objetivo de estas evaluaciones de impacto es averiguar cómo nuestras actividades/relaciones comerciales y productos/servicios impactan en los derechos humanos existentes (ver asuntos de derechos humanos analizados en evaluaciones en impacto en gráfica) y, sobre esta base, identificar los asuntos de derechos humanos más relevantes para nuestra actividad empresarial. Se llevan a cabo evaluaciones adicionales y específicas sobre cual-

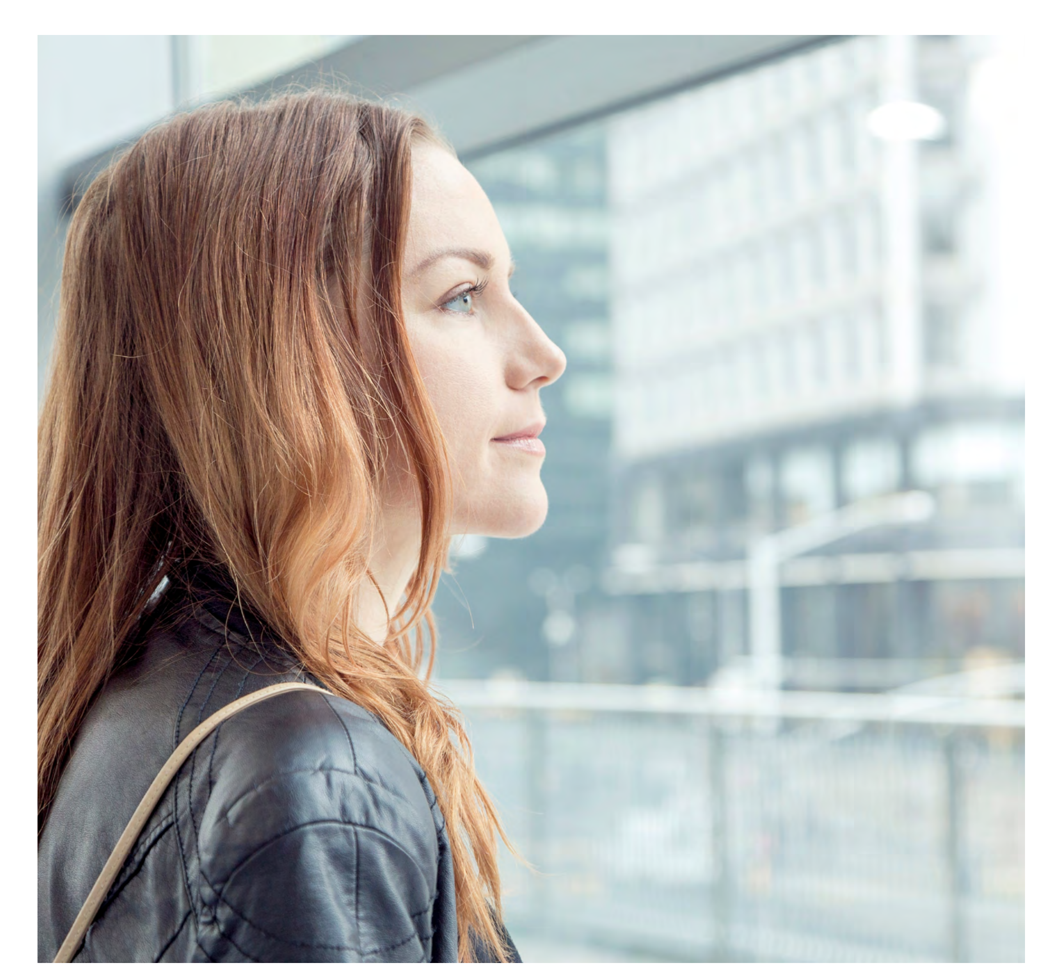
Asuntos de derechos humano	Abolición del trabajo infantil/forzado; Condiciones laborales; No-Discriminación; Privacidad; Protección del medio ambiente; Diversidad/ Inclusión; Acceso a la Información; Libertad de Expresión
Cadena de valor	Proveedores — Upstream — Telefónica — Downstream — Clientes
Politicas internas	Política de Sostenibilidad en la Cadena de Suministro; Política de Seguridad y Salud; Política de Diversidad; Política de Seguridad; Reglamento de Peticiones por parte de Autoridades Competentes; Environmental Policy; Política Anti-Corrupción; Política de Privacidad; Compromiso con la protección de menores; Política de No-Discriminación; Principios de IA; Política de Comunicación Responsable

Política de derechos humanos — Principios de negocio responsable

Foco: Privacidad y Libertad de Expresión dentro de la Debida Diligencia en Derechos Humanos





quier tema relevante en el que en la evaluación de impacto se haya detectado especial preocupación. Además, se llevan a cabo evaluaciones de impacto locales en los países en los que operamos para integrar el contexto local en la evaluación general. Además, contamos con un mecanismo de reclamación y remedio, nuestro Canal de Negocio Responsable, que permite a los grupos de interés, de forma confidencial y anónima, plantear quejas o consultas (en varios idiomas) sobre cualquier aspecto relacionado con los Principios de Negocio Responsable, explícitamente también sobre derechos humanos en general y privacidad y/o libertad de expresión en particular. Contamos con un procedimiento que garantiza el adecuado funcionamiento del Canal.

En 2013, de la mano de *Business for Social Responsability* (BSR), realizamos nuestra primera evaluación de impacto en todas nuestras operaciones. La privacidad y la libertad de expresión fueron identificados como dos asuntos a gestionar dentro de la matriz y publicamos nuestro compromiso específico en derechos humanos. En 2019 actualizamos nuestra matriz de impacto con una nueva evaluación de la mano de *Business & Human Rights* (BHR) con el objetivo de comprender los impactos potenciales derivados de nuestra estrategia, de las nuevas actividades del Grupo y de un entorno digital en constante cambio. Los derechos de privacidad y libertad de expresión fueron otra vez identificados como relevantes (ver nuestra web sobre derechos humanos para obtener más información sobre la última evaluación de impacto a nivel global). Una vez concluido el análisis, se identificaron varias actividades y temáticas que merecían una evaluación específica como han sido la evaluación de impacto en el proceso de despliegue de red, en el desarrollo de nuevos productos y servicios –incluidos aquellos en los que se aplique la Inteligencia Artificial–, y en los derechos de niños, niñas y adolescentes.

El conjunto de todo este proceso en torno a las evaluaciones de impacto forma la base para adaptar nuestras políticas/ procesos internos con vistas a prevenir, mitigar y/o remediar los posibles impactos sobre los derechos humanos en general y sobre la privacidad y libertad de expresión en particular. A continuación, destacamos las políticas/ procesos internos más importantes en materia de privacidad y libertad de expresión que se han adaptado a raíz de las ultimas evaluaciones de impacto.

Políticas y procesos de aplicación

Hemos impulsado y revisado diferentes políticas y procedimientos para asegurar la protección de los derechos de privacidad y libertad de expresión, el acceso a la información y la no-discriminación.

Política Global de Derechos Humanos:
Aprobada en el 2019, esta política formaliza nuestro compromiso con los derechos humanos recogido, de forma general, en los Principios de Negocio Responsable de Telefónica, y de forma más específica en un conjunto de políticas y normas que velan por el respeto y aplicación de derechos humanos sociales, económicos y culturales internacionalmente reconocidos.

Política de Privacidad:
Actualizada en el 2018, forma parte de la estrategia de Telefónica para diseñar una nueva experiencia digital basada en la confianza (Confianza Digital).

Consciente de la importancia de merecer la confianza de nuestros clientes y/o usuarios y, con carácter general, de nuestros grupos de interés, esta política les garantiza el control sobre y el valor de sus datos personales cuando son objeto de tratamiento por Telefónica.

Establece unas normas de comportamiento común obligatorias para todas las entidades del Grupo, y establece un marco para una cultura de privacidad basada en los principios de licitud, transparencia, compromiso con los derechos de los interesados, seguridad y limitación del plazo de conservación.

Bajo el principio de transparencia garantizamos que a los interesados se les facilite de forma accesible e inteligible información sobre los datos personales que recogemos (tales como, a título de ejemplo, nombre, apellidos, dirección, cuenta bancaria, preferencias personales etc..), cómo los recogemos, la finalidad (prestación del servicio, etc..).

Reglamento de Modelo de Gobierno de Protección de Datos:
Tiene por objetivo englobar los aspectos más importantes a tener en cuenta para una correcta gestión y protección de los datos de carácter personal.

Se establece un modelo organizativo y de relación donde el máximo responsable de la Función de Protección de Datos Personales es el Delegado de Protección de Datos (DPO), quien reporta directamente al Consejo de Administración de Telefónica, S.A. Además, se articula a través de una estructura de relacionamiento y gobierno:

- **Oficina DPO:** Encargada de la coordinación de Cumplimiento y Datos (asegurar la ejecución global de cumplimiento de todo el Grupo) y una función técnica de Protección de Datos encargada de la supervisión del cumplimiento de la normativa de protección de datos del Grupo Telefónica.
- **Comité de Seguimiento:** Cuenta con la representación de diferentes áreas de la Compañía (Seguridad, Secretaría General, Regulación, Tecnología, CDO, Cumplimiento, Ética y Sostenibilidad y Auditoría Interna). Se revisa el estado general de cumplimiento del modelo de gobierno.
- **Comités de Negocio:** La Oficina DPO mantiene a través de la función técnica de Protección de Datos, interacciones permanentes con otras áreas, a través de los Responsables de Cumplimiento, al objeto de asegurar la máxima uniformidad en la aplicación de los procesos comunes, y/o la identificación y tratamiento de problemáticas específicas de privacidad en el ámbito de actividad de cada área.

Reglamento ante Peticiones por parte de las Autoridades Competentes:
En el 2019 se aprobó el Reglamento para reforzar el procedimiento ya existente desde 2016, con el objetivo de alinearlo con otras Políticas existentes y nuestros compromiso por el respeto a los derechos y libertades fundamentales. Define los principios y directrices mínimas que deben ser contemplados en los procedimientos internos propios de cada una de las compañías del Grupo/ Unidades de Negocio/OB para cumplir con su deber de colaboración con las Autoridades Competentes de acuerdo con cada legislación nacional y con los derechos fundamentales de los interesados en este tipo de procedimientos.

Los principios que rigen el proceso son Confidencialidad, Exhaustividad, Fundamentación, Proporcionalidad, Neutralidad Política, Respuesta Diligente y Seguridad.

Nuestro compromiso es asegurar la participación en el proceso de áreas legales o áreas similares con competencias legales en la recepción de las solicitudes. Contamos con interlocutores fijos como ventanilla única en nuestra relación con las Autoridades Competentes, de manera que rechazamos cualquier solicitud que no viene por este conducto reglamentario.

Política Global de Seguridad:

Actualizada en el 2019 e inspirada en los principios de 'honestidad y confianza', esta política se rige por los estándares y regulaciones nacionales e internacionales en la materia, y establece los principios rectores en materia de seguridad que resultan aplicables a todas las empresas que integran el Grupo Telefónica.
Las actividades de seguridad se rigen por los siguientes Principios:

> **Legalidad:** Necesario cumplimiento de las leyes y regulaciones, nacionales e internacionales, en materia de seguridad.

> **Eficiencia:** Se destaca el carácter anticipativo y preventivo sobre cualquier potencial riesgo y/o amenaza con el objetivo de adelantarse y prevenir cualquier potencial efecto dañino y/o mitigar los perjuicios que pudieran causarse.

> **Corresponsabilidad:** El deber de los usuarios de preservar la seguridad de los activos que Telefónica pone a su disposición.

> **Cooperación y Coordinación:** Para alcanzar los niveles de eficiencia se prioriza la cooperación y la coordinación entre todas las unidades de negocio y empleados.

Fruto de esta Política durante el 2019 -2020 se actualizaron varias normativas de desarrollo para el efectivo cumplimiento de la misma. (Reglamento Gestión de Incidentes y Emergencias; Reglamento Análisis de Riesgos de Seguridad; Reglamento Seguridad en Redes y Comunicaciones; Reglamento de Ciberseguridad; Reglamento Seguridad en la Cadena de Suministro y el Reglamento Gobierno de la Seguridad entre otras.)

Política de Comunicación Responsable:

Aprobada en octubre del 2018, tiene por objetivo establecer las pautas de actuación para Telefónica en torno a nuestros canales de comunicación y generación de contenidos. Se basa en los Principios de Legalidad, Integridad y Transparencia, Neutralidad y Protección de Menores.

En el principio de neutralidad nos comprometemos a evitar posicionarnos políticamente como Compañía y promovemos el derecho a la libertad de expresión, dentro de los marcos regulatorios a los que estamos sometidos. En nuestra comunicación hacia clientes y a través de la publicidad prohibimos ciertas conductas que van en contra de nuestros Principios de Negocio Responsable. Así, en nuestros mensajes y nuestros patrocinios no toleramos que se abuse de la buena fe del consumidor, que atenten contra la dignidad de las personas, que fomenten el consumo del alcohol, el tabaco, las drogas, los trastornos alimenticios o el terrorismo, que inciten al odio, a la violencia o a la discriminación, a la comisión de comportamientos ilegales y puedan abusar de la ingenuidad del menor.

Principios de Inteligencia Artificial:

Aprobados por el Comité Ejecutivo en octubre del 2018, nos comprometemos a diseñar, desarrollar y usar la Inteligencia Artificial con Integridad y Transparencia. Son principios que sitúan a las personas en el centro y garantizan el respeto de los derechos humanos en cualquier entorno y proceso en el que se use la Inteligencia: Hacen hincapié en la igualdad e imparcialidad, la transparencia, la claridad, la privacidad y la seguridad. Son normas que aplican en todos los mercados en los que operamos y se extienden a toda nuestra cadena de valor, a través de socios y proveedores.

Durante el 2019, hemos estado trabajando en la implementación de estos principios en todas nuestras operaciones, centrándonos en tres pilares interrelacionados:

> **Formación para empleados:** contamos con un curso de formación sobre Ética e Inteligencia Artificial para nuestros empleados, explicando a) cómo la Inteligencia Artificial, si se utiliza de forma inapropiada, puede tener un impacto negativo en los derechos humanos y b) qué pasos se deben tomar en la práctica para hacer frente a los posibles riesgos en materia de derechos humanos asociados con el uso de la Inteligencia Artificial.

> **Cuestionario de autoevaluación** para los jefes de producto que compran, desarrollan y/o usan Inteligencia Artificial. Así,para cada uno de los principios se elaboran preguntas relacionadas con los algoritmos utilizados y pueden identificar los riesgos asociados a los principios y las recomendaciones para prevenirlos o evitar esos riesgos.

> **Gobernanza:** Contamos con un modelo de gobernanza para la implementación efectiva de los Principios

Formación en derechos humanos:

A finales del 2019 empezamos a trabajar a nivel global la formación en derechos humanos. Así, profundizamos durante el 2020 y habrá una sección más ampliada sobre derechos humanos dentro del curso obligatorio de los Principios de Negocio Responsable y talleres específicos para empleados cuyo trabajo puede tener un impacto mayor en los derechos humanos. Las áreas a las que se impartirán estos talleres serán:

> **Jurídica y Cumplimiento:** Para los asuntos de Privacidad y Libertad de Expresión desde una perspectiva de derechos humanos, haciendo hincapié en los principios del GNI y de los requerimientos de las Autoridades Competentes y sobre los derechos humanos a tener en cuenta en los acuerdos de fusión, adquisición y desinversión.

> **Asuntos Públicos y Relaciones Institucionales:** Para promover la privacidad y la libertad de expresión a través de un *advocacy* proactivo con los grupos de interés externos (por ejemplo gobiernos, organizaciones internacionales, ONGs).

> **Gestores de producto y desarrolladores:** Para la integración de los derechos humanos desde el diseño y haciendo foco en los productos y servicios que incorporan nuevas tecnologías o Inteligencia Artificial.

Riesgo básico de derechos humanos:

Los riesgos relacionados con impactos en derechos humanos siempre han estado presentes en el modelo de levantamiento de riesgos de Telefónica, sin embargo, en el 2017 se incluyó de forma específica el riesgo básico de derechos humanos.

El objetivo es levantar cualquier riesgo de impacto, directo o indirecto, en las operaciones del Grupo Telefónica debido a posibles vulneraciones de derechos humanos, como consecuencia de la propia actividad de la Compañía o de la actividad que llevan a cabo nuestros proveedores u otras relaciones comerciales. Este análisis contempla cualquier cambio legislativo en los países o de actividad que pueda tener un impacto en los derechos humanos.

Este levantamiento de riesgos facilita definir las pautas de actuación necesarias en las operaciones directamente afectadas con el objetivo de mitigar y/o evitar estos riesgos y priorizar las actuaciones de Auditoría Interna, de cara a su planificación de actividades de supervisión de las estructuras de control interno.

Derechos humanos por diseño:

Evaluamos los posibles impactos en los derechos humanos de nuevos productos y servicios a través del enfoque 'derechos humanos desde el diseño', es decir, desde el inicio del diseño y/o comercialización de productos y servicios. Concretamente, los jefes de producto deben llevar a cabo una autoevaluación de nuevos productos y servicios a través de una herramienta en línea en la fase de diseño con el fin de identificar y abordar los posibles impactos en los derechos humanos ya en la fase de diseño. Los derechos humanos abordados en este cuestionario son, por ejemplo, privacidad, libertad de expresión, no- discriminación, Inteligencia Artificial, impacto en grupos vulnerables como los menores, etcétera. Si se identifican riesgos en materia de derechos humanos una vez finalizada la autoevaluación, el producto/servicio en cuestión se somete a un análisis más detallado con la ayuda de expertos en derechos humanos de la empresa, a fin de abordar los posibles efectos adversos sobre los derechos humanos en el desarrollo del producto/servicio en el futuro.

Iniciativas de Transparencia:

Uno de los retos y elementos clave en la privacidad es garantizar la transparencia y en Telefónica hemos apostado por llevarlo a la práctica incluyéndolo como uno de los Principios de la Política Global de Privacidad y desarrollando diferentes iniciativas que implementan este Principio como son, como son el Centro de Privacidad Global y los Centros de Privacidad de las operadoras. Además, Telefónica comienza a disponibilizar a clientes el acceso a los datos que generan durante el uso de nuestros servicios, datos que son recogidos en el denominado “Personal Data Space". Durante el 2020 se lanzará el Centro de Transparencia en España, que hace realidad la consulta y gestión de los datos recogidos en el Personal Data Space. A través de la sección “Permisos” los clientes pueden gestionar sus consentimientos sobre el uso de datos para determinados propósitos. Y desde la sección de “Consulta y Descarga” se ofrecen útiles visualizaciones de diferentes tipos de datos, con una experiencia amigable y respetando los criterios de privacidad, con la opción de descargar un documento con mayor nivel de detalle de esos conjuntos de datos.

La experiencia del Centro de Transparencia se ha diseñado centrada en el usuario, evitando emplear un lenguaje legal complejo, donde Aura, la Inteligencia Artificial de Telefónica, acompaña y aporta en cada visualización una explicación sobre el propósito y la naturaleza de esos datos dentro de Telefónica, ofreciendo claridad, transparencia, y reforzando la confianza.

Con el Centro de Transparencia empoderamos a nuestros clientes con funciones de control y transparencia sobre sus datos.

Aplicación efectiva de las políticas y procesos:

De acuerdo con nuestra Política de Elaboración y Organización del Marco normativo, corresponde a la dirección de Auditoría Interna la coordinación del Marco Normativo del Grupo Telefónica, a través de la supervisión del proceso de definición de las normas Internas; promoviendo, a su vez, acciones que favorezcan la actualización y comunicación de las mismas. Adicionalmente detecta las necesidades y oportunidades de mejora, modificación o actualización de las Normas Internas existentes, proponiendo líneas de actuación a los Responsables de las Normas Internas, y proporcionar apoyo y asesoramiento al Responsable de la Norma Interna en relación con su redacción e implantación.

La observancia y cumplimiento de la normativa (p. ej. las políticas de privacidad, seguridad etc. mencionadas) son objeto de revisión y supervisión por parte de los responsables de las Normas Internas que lideran la propuesta, creación, difusión e implantación de la Norma interna y realizan su seguimiento, evaluación y actualización, quien está facultada para realizar las supervisiones muestrales de los controles siempre que lo considere conveniente.



GNI (Global Network Initiative) y RDR (Ranking Digital Rights)

Como muestra de nuestro compromiso con los derechos fundamentales de la libertad de expresión y la privacidad, somos miembros constituyentes del Grupo de Diálogo de la Industria de Telecomunicaciones para la Libertad de Expresión y la Privacidad (TID), grupo que se fusionó con el *Global Network Initiative* (GNI) en 2017. El GNI es una organización de escala global e la que son miembros inversores, think tanks y sociedad civil y compañías privadas: operadores de telecomunicaciones, proveedores de servicios sobre internet, y fabricantes de equipos y software.

Como miembros de GNI, Telefónica es una de las empresas firmantes de los principios del sector de las comunicaciones sobre libertad de expresión y privacidad y asumimos el compromiso de su implementación y rendición de cuentas mediante evaluaciones de cumplimiento por parte de asesores independientes. Así en el 2019, hemos pasado con éxito nuestro primer proceso de evaluación independiente del GNI. El Consejo de Administración del GNI, integrado por múltiples grupos de interés, determinó que Telefónica está realizando esfuerzos de buena fe para implementar los principios del GNI sobre la libertad de expresión y privacidad con mejoras a lo largo del tiempo. La evaluación positiva del GNI se basó en un informe de un asesor externo independiente (Deloitte) que evaluó las políticas, los procesos, y el modelo de gobernanza de Telefónica para salvaguardar la libertad de expresión y la privacidad de sus clientes.

Además, quedamos primeros entre todas las empresas de telecomunicaciones en la edición 2019 del Ranking *Digital Rights*, que evalúa los compromisos, políticas y prácticas de las empresas que afectan a la libertad de expresión y a la privacidad de los clientes, incluidos los mecanismos de gobernanza y supervisión.



Indicadores de este Informe

En los apartados siguientes reportamos el número de solicitudes que recibimos por parte de las autoridades nacionales competentes en los países donde operamos.

Cualquier solicitud que se pueda recibir por parte de una autoridad competente nacional debe cumplir con los procesos judiciales y/o legales que corresponda a cada país. En Telefónica solo atendemos solicitudes que provengan de una autoridad nacional competente siguiendo nuestro Reglamento ante Peticiones por parte de las Autoridades Competentes. En Telefónica **no atendemos solicitudes privadas,** solo se tramitan las solicitudes que provienen de autoridades determinadas por ley. Dicho esto y como única excepción, en la lucha proactiva contra los contenidos de imágenes de abusos sexuales a menores de edad en la Red, Telefónica procede al bloqueo de estos materiales siguiendo las pautas y las listas proporcionadas por la Internet Watch Foundation.

Los indicadores que reportamos son:

- **Interceptaciones legales:** Aquellas solicitudes que proceden de las Autoridades Competentes en el marco de investigaciones criminales y, en su caso, civiles con el objetivo de interceptar comunicaciones o acceder a datos de tráfico en tiempo real.
  Este año hemos incorporado el desglose de Interceptaciones siempre y cuando sea técnicamente y/o legalmente posible, por:
  - Altas: Solicitudes de una nueva interceptación.
  - Prórrogas: Solicitudes para prorrogar una interceptación ya existente.
  - Bajas: Solicitudes para desconectar a una interceptación existente.
- **Metadatos asociados a las comunicaciones:** Aquellas solicitudes procedentes de las Autoridades Competentes que tienen por objetivo obtener datos históricos referidos a:
  - el nombre y dirección del usuario registrado (datos de abonado);
  - los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet);
  - la fecha, hora y duración de una comunicación;
  - el tipo de comunicación;
  - la identidad de los equipos de comunicación (incluyendo IMSI o IMEI);
  - la localización del usuario o del dispositivo.
- **Bloqueo y restricción de contenidos**: Aquellas solicitudes de las Autoridades Competentes para bloquear el acceso a sitios web específicos o a un determinado contenido.
  Se trata de solicitudes para bloquear el acceso a un sitio web o a un contenido, no una petición para eliminar el contenido del usuario.
  A título de ejemplo, las demandas de bloqueo se emiten porque los sitios web o determinados contenidos que publican son contrarios a las leyes locales (suelen estar relacionados con material de abuso sexual infantil, los juegos de azar online, violación de derechos de autor, difamación, venta ilegal de medicamentos, armas, marca comercial, etc.).
  Este año hemos incorporado el desglose por tipo de bloqueo, cuando las herramientas y la legislación lo permiten.
- **Suspensiones geográficas o temporales de servicio:** Aquellas solicitudes requerimiento de las Autoridades Competentes para limitar temporal y/o geográficamente la prestación de un servicio. Estos requerimientos suelen estar relacionados con situaciones de fuerza o causa mayor como catástrofes naturales, actos de terrorismo, etc.

Además, para cada indicador reportamos también los siguientes subindicadores:

- **Solicitudes rechazadas o atendidas parcialmente:** número de veces que hemos rechazado una solicitud o que solo hemos proporcionado información parcial o ninguna información en respuesta a una solicitud por alguna de las siguientes razones:
  - Por no ajustarse a la legislación local para ese tipo de requerimiento.
  - Por no contener todos los elementos necesarios que posibilita la ejecución (firmas necesarias, autoridad competente, descripción técnica del requerimientos etc...)
  - Porque técnicamente es imposible ejecutar el requerimiento.

- **Accesos afectados:** número de accesos que se ven afectados por cada solicitud. Para bloqueo y restricción de contenidos contabilizamos Url's afectadas.

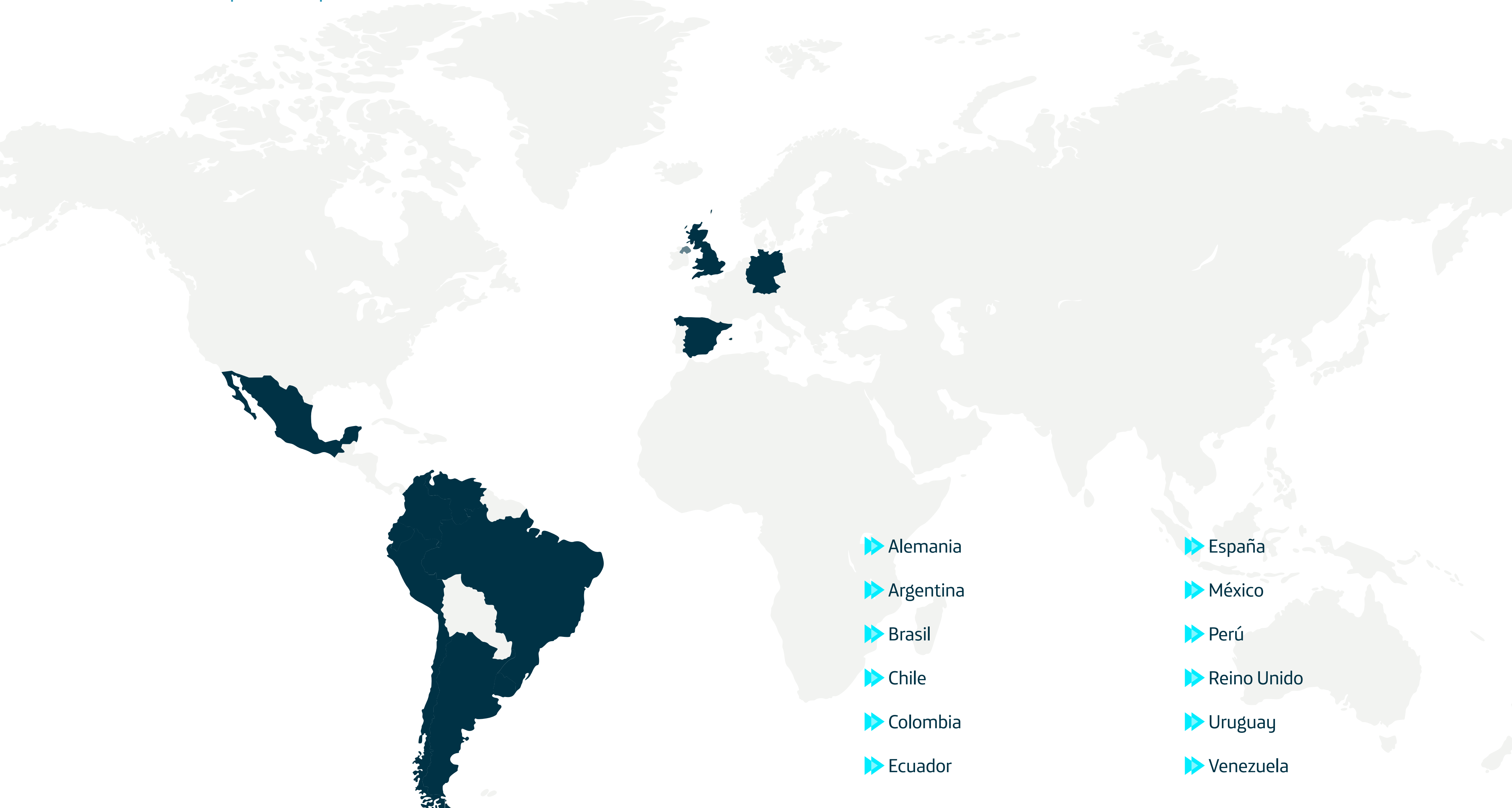
Por otra parte, en este Informe de Transparencia, nuestro objetivo es informar de forma transparente sobre nuestros esfuerzos en relación con las peticiones o solicitudes con potencial impacto relevante sobre el derecho a la libertad de expresión y derecho a la privacidad en las telecomunicaciones. Identificamos dicha solicitud y demandas como *major events.*

A este respecto cabe destacar en España la Modificación de la Ley 9/2014, General de Telecomunicaciones, en virtud de lo establecido en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Dicha ley y los artículos que afectan a Interceptación legal se detallan en el contexto legal del Informe de España.

También debemos destacar la situación de excepcionalidad en la que continúa Venezuela y los retos a los que nos enfrentamos para la verificación de nuestros procesos globales en el país. En esta situación, Telefónica debe priorizar el cumplimiento con la legislación vigente, el mantenimiento de la conectividad en el país y el bienestar de nuestros empleados.



Informe por país



Alemania

www.telefonica.de

Telefónica cuenta con un largo historial en Alemania y opera bajo la marca comercial O2.

Telefónica Deutschland ofrece telefonía móvil de pre-pago y contrato a clientes residenciales y empresas, e innovadores servicios de datos a través de las tecnologías GPRS, UMTS y LTE. Como proveedor integrado de comunicación, también ofrece servicios de ADSL e internet de alta velocidad. Telefónica cuenta con un total de 48,2 millones de accesos en Alemania.

Los ingresos totales de Telefónica en Alemania se sitúan en 7.399 millones de euros y el OIBDA en 2.326 millones de euros.

48.258
Accesos totales

Accesos a cierre de 2019 (datos en miles).





Accesos

2.129 Telefonía fija	**43.827** Telefonía móvil
2.302 Datos e Internet	**0,0** TV de pago

Accesos a cierre de 2019 (datos en miles).

INTERCEPTACIÓN LEGAL

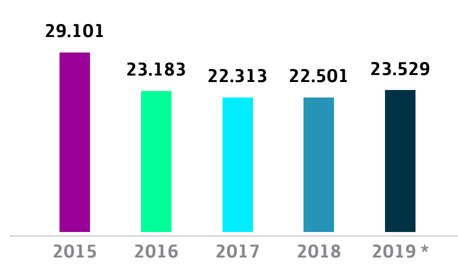
Contexto legal

- Ley de Telecomunicaciones– Seccion 110 (*Telekommunikationsgesetz* - TKG).
- Código de Procedimiento Penal (StPO *The German Code of Criminal Procedure*).
- Sección 100 a Ley articulo 10 G10 (*Artikel 10 Gesetz - G10*).
- Ley de servicios de investigaciones aduaneras (ZFDG)
- Ley federal de la oficina de policía penal (BKAG).
- Leyes policiales de los estados federales (*Landespolizeigesetze*).

Autoridades Competentes

- Agencias y Cuerpos de Seguridad del Estado (*Law Enforcement Agencies*-LEAs) como autoridades policiales (nacional y federal) y servicios de inteligencia y aduanas (nacional y federal).
- Las medidas recogidas en la Sec. 100a del Código de Procedimiento Penal alemán (StPO) requieren una orden judicial previa. En caso de circunstancias extremas, el Ministerio Público podrá emitir una orden, que deberá ser confirmada por un Juzgado dentro de los tres días hábiles siguientes para que resulte eficaz.

Solicitudes*



* El volumen total incluye nuevas, prorrogas y cese de interceptaciones,

Accesos afectados	55.772	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

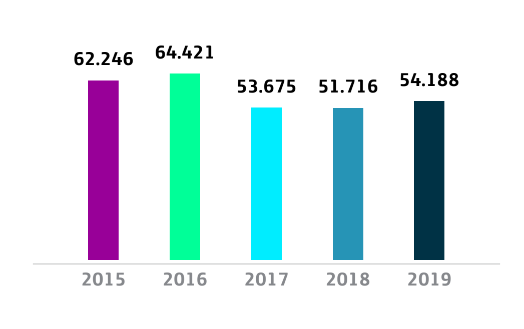
Contexto legal

- Ley de Telecomunicaciones Aleman Sec. 96, 113b (*Telekommunikationsgesetz* - TKG).
- Código de Procedimiento Penal Sec. 100g (*Strafprozessordnung* – StPO).
- Leyes policiales de los estados federales (*Landespolizeigesetze*).

Autoridades Competentes

- Agencias y Cuerpos de Seguridad del Estado (*Law Enforcement Agencies*-LEAs) como autoridades policiales (nacional y federal) y servicios de inteligencia y aduanas (nacional y federal).
- Las medidas recogidas en la Sec. 100a del Código de Procedimiento Penal alemán (StPO) requieren una orden judicial previa. En caso de circunstancias extremas, el Ministerio Público podrá emitir una orden, que deberá ser confirmada por el Juzgado dentro de los tres días hábiles siguientes para que resulte eficaz.

Solicitudes



Accesos afectados	458.872	Solicitudes rechazadas	0



BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

No existen leyes en el marco regulatorio que permitan bloqueo o filtrado de contenidos.

Autoridades Competentes

No aplica.

Solicitudes

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

URL afectadas **N/A**

Solicitudes rechazadas **N/A**

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

Autoridades Competentes

No aplica.

Solicitudes

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

Accesos afectados **N/A**

Solicitudes rechazadas **N/A**



Argentina

www.telefonica.com.ar

Telefónica está presente en Argentina desde la privatización de los servicios telefónicos en 1990. A lo largo de estos años, la compañía se ha convertido como un grupo líder de empresas especializado en telecomunicaciones integradas.

Tras haber sido la primera inversión significativa de capitales españoles, contribuyó en estos años al desarrollo de las comunicaciones mediante inversiones de infraestructuras y una amplia oferta de servicios de telefonía fija, móvil e Internet.

Telefónica en Argentina gestiona más de 21,2 millones de accesos a diciembre de 2019.

Respecto a las cifras financieras, los ingresos de Telefónica en Argentina alcanzaron 2.163 millones de euros y el OIBDA sumó 499 millones de euros.

21.221
Accesos totales

Accesos a cierre de 2019 (datos en miles).



Accesos

3.143 Telefonía fija	**16.538** Telefonía móvil
1.371 Datos e Internet	**153,2** TV de pago

Accesos a cierre de 2019 (datos en miles).

INTERCEPTACIÓN LEGAL

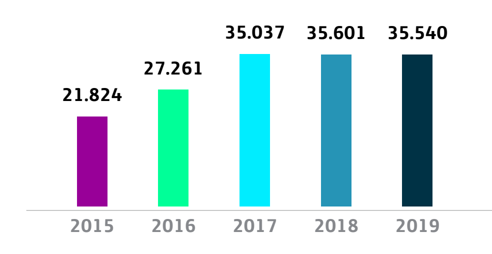
Contexto legal

- Constitución Nacional Argentina (Artículo 18).
- Ley 19.798 (arts. 18 y 19): Inviolabilidad de las comunicaciones.
- Ley 27.078, art. 5: Inviolabilidad de las comunicaciones.

Autoridades Competentes

- Son los jueces los únicos autorizados a solicitar la intervención judicial sobre un acceso, y los Fiscales únicamente en caso de tratarse de un delito de Secuestro Extorsivo en curso, en cuyo supuesto podrán solicitar la intervención, debiendo ser ratificada por un juez en un plazo máximo de 24 horas. En cuanto al procedimiento, los juzgados solicitan la intervención a la denominada Dirección de Asistencia Judicial en Delitos Complejos (DAJDECO), organismo dependiente de la Corte Suprema de Justicia de la Nación, quienes luego formalizan y dan curso el pedido de intervención a las empresas prestatarias de servicios.

Solicitudes



Desglose de Interceptaciones (2019)



Altas	14.727
Prórrogas	6.328
Bajas	14.485

Accesos afectados	14.727	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

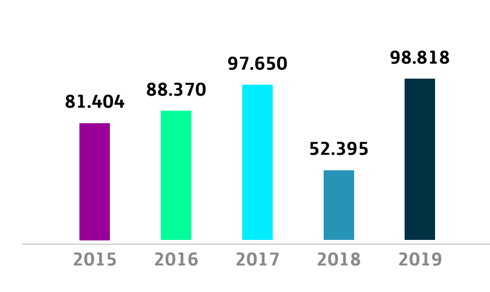
Contexto legal

- Constitución Nacional Argentina (Artículo 18).
- Ley 19.798 (arts. 18 y 19): Inviolabilidad de las comunicaciones.
- Ley 27.078, art. 5: Inviolabilidad de las comunicaciones.

Autoridades Competentes

- Jueces, Fiscales y los cuerpos y fuerzas de seguridad del Estado al que se le haya delegado la investigación.

Solicitudes



*En el 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada y no agregada como en años anteriores por lo que no es un dato comparable con el resto.

Accesos afectados	98.818	Solicitudes rechazadas	0

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

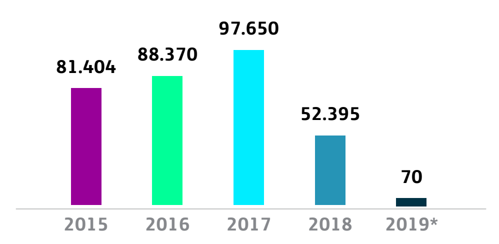
Contexto legal

Ley 27.078, art. 5.: Inviolabilidad de las comunicaciones.

Autoridades Competentes

- Jueces, Fiscales y los cuerpos y fuerzas de seguridad del Estado al que se le haya delegado la investigación.

Solicitudes



*En el 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada y no agregada como en años anteriores, por lo que no es un dato comparable con el resto.

Tipo de bloqueos	Apuestas on line		
URL afectadas	68	Solicitudes rechazadas	0

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

Si bien no existe una norma específica que lo regule, podría interpretarse que forma parte de lo establecido en el Art. 57 de la Ley 27.078, en cuanto dispone;

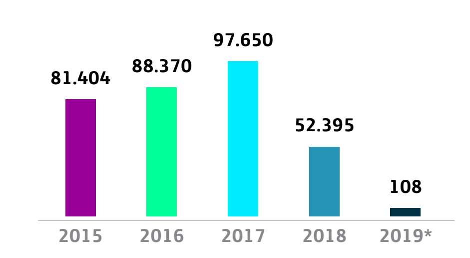
ARTÍCULO 57. — Neutralidad de red. Prohibiciones. Los prestadores de Servicios de TIC no podrán:

a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.

Autoridades Competentes

Al no haber una norma específica, el único órgano competente para dictar una medida de suspensión del servicio en una determinada zona es un juez con competencia federal.

Solicitudes



*En el 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada y no agregada como en años anteriores, por lo que no es un dato comparable con el resto. Corresponden a solicitudes para restringir temporalmente el tráfico de datos móviles de determinados clientes.

Accesos afectados	108	Solicitudes rechazadas	0



Brasil

www.telefonica.com.br

Telefónica entró en el mercado brasileño en 1998, momento en el que se estaba produciendo la reestructuración y privatización de Telebrás. Más adelante, en el año 2002, Telefónica y Portugal Telecom crean una Joint Venture para operar en el mercado móvil brasileño e inician sus operaciones comerciales con el nombre de Vivo en abril de 2003.

Durante el año 2015, se cerró la adquisición de GVT, lo que sitúa a Telefónica Brasil como el operador integrado líder del mercado brasileño.

Telefónica en Brasil gestiona más de 93,7 millones de accesos a diciembre de 2019.

Respecto a las cifras financieras, los ingresos de Telefónica en Brasil alcanzado los 10.035 millones de euros y el OIBDA, 4.262 millones de euros



93.732,3
Accesos totales

Accesos a cierre de 2019 (datos en miles).



Accesos

10.817,0 Telefonía fija	**74.573,1** Telefonía móvil
7.009,2 Datos e Internet	**1.319,7** TV de pago

Accesos a cierre. 2019 (datos en miles)



INTERCEPTACIÓN LEGAL

Contexto legal

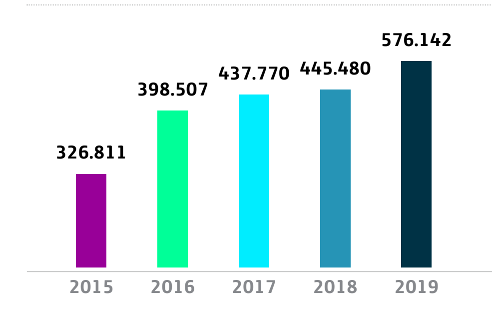
- Constitución de la República Federal de Brasil: Art. 5º.
- Ley Nº 9.296, de 24 de julio de 1996.
- Resolución N º 426 del 9 de diciembre de 2005 / Reglamento de Servicio de Telefonía Fija - STFC. STFC.
- Resolución N º 614 del 28 de mayo 2013/ Reglamento de Servicio de Comunicación Multimedia.
- Resolución N º 477 del 7 de agosto de 2007/ Reglamento de Servicio Móvil Personal - SMP.

.

Autoridades Competentes

- De acuerdo con el artículo 3º de la Ley Federal brasileña n. 9.296/1996 (Ley de las Interceptaciones), solamente el Juez (de la esfera criminal) puede determinar las interceptaciones (telefónicas y telemáticas), a petición de la Fiscalía (*Ministério Público*) o Comisario de Policía (*Autoridade Policial*).

Solicitudes



Desglose de Interceptaciones (2019)



Altas	556.520*
Prórrogas	-
Bajas	19.622

*Se incluyen altas y prórrogas de interceptaciones.

Accesos afectados	556.520	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

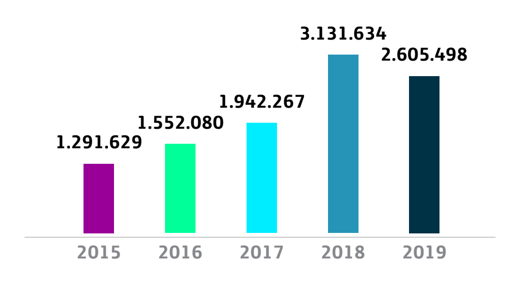
Contexto legal

- Ley Nº 9.296, de 24 de Julio de 1996.
- Ley Nº 9.472, de 16 de julio de 1997. Art. 3.
- Ley Nº 12.683, de 9 de julio de 2012. Art. 17-B.
- Ley Nº 12.830, de 20 de junio de 2013. Art. 2.
- Ley Nº 12850 de 20 de agosto de 2013. Art. 15.
- Ley Nº 12965 de 23 de abril de 2014. Art. 7; 10 y 19.
- DECRETO Nº 8.771, de 11 de mayo de 2016. Art. 11.
- Ley N.º 13344, de octubre de 2016. Art. 11.
- Ley N.º 13812, de mayo de 2019. Art. 10.
- Resolución N º 426 del 9 de diciembre de 2005 / Reglamento de Servicio de Telefonía Fija - STFC. STFC. Art. 11; 22; 23 y 24.
- Resolución N º 477 del 7 de agosto de 2007/ Reglamento de Servicio Móvil Personal - SMP. Art. 6;10 ;12;13; 89 y 90.
- Resolución N º 614 del 28 de mayo 2013/ Reglamento de Servicio de Comunicación Multimedia. Art. 52 y 53.

Autoridades Competentes

- Fiscalía, Comisarios de Policía y Jueces de cualquier esfera, como también Presidentes de las Comisiones Parlamentarias de Investigación: el nombre y dirección del usuario registrado (datos de abonado), así como la identidad de los equipos de comunicación (incluyendo IMSI o IMEI).
- Jueces de cualquier esfera: los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet), la fecha, hora y duración de una comunicación y la localización del dispositivo.

Solicitudes



Accesos afectados	2.605.498	Solicitudes rechazadas	0

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

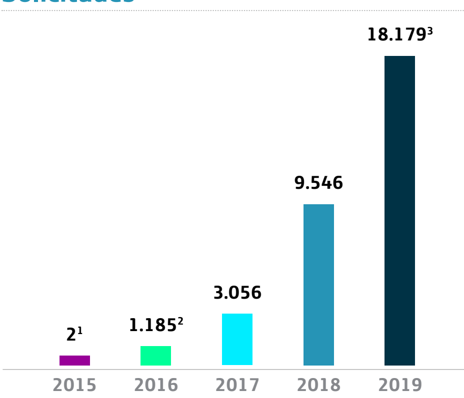
Contexto legal

Ley Nº 12965 de 23 de abril de 2014. Art. 7 y 19.

Autoridades Competentes

Exclusivamente Jueces

Solicitudes



URL afectadas	18.179	Solicitudes rechazadas	0

Derechos de Autor	Derechos de Imagen
0,03%	0,07%

Ejecución de deuda	Piratería
0,01%	99,88%

Otros
0,02%

1. Los dos casos de 2015 corresponden al bloqueo de la Aplicación Whastap.
 * En febrero de 2015, la autoridad judicial determinó que las operadoras bloquearan el acceso de sus clientes al aplicación WhatsApp hasta el cumplimiento de la orden original enviada a a la aplicación. El requerimiento tenía fundamento legal en el ámbito de procedimientos criminales llevados a cabo por la Comisaria de Protección al Niño y al Adolescente.
 ** En 16/12/2015, la compañía recibió otra orden, por un período de acceso de 48 horas a la aplicación WhatsApp. La medida fue adoptada con la misma base legal que el caso mencionado en el punto anterior.

2. Aclaración: Pasadas las medidas de bloqueos generales que afectaron a todos los clientes en potencial (caso whatsapp), las autoridades públicas empezaron a practicar bloqueos individuales en el ámbito de investigaciones criminales.
3. En el 2019 se contabilizan solo bloqueo de URL's dejando las suspensiones del servicios de cuentas individuales en el indicador 'Suspensión del Servicio'.

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

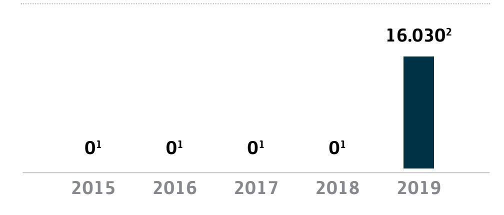
Contexto legal

- Resolución nº 73 de 25 de noviembre de 1998. Art. 31
- Resolución nº 477 de 7 de agosto de 2007. Art. 19

.Autoridades Competentes

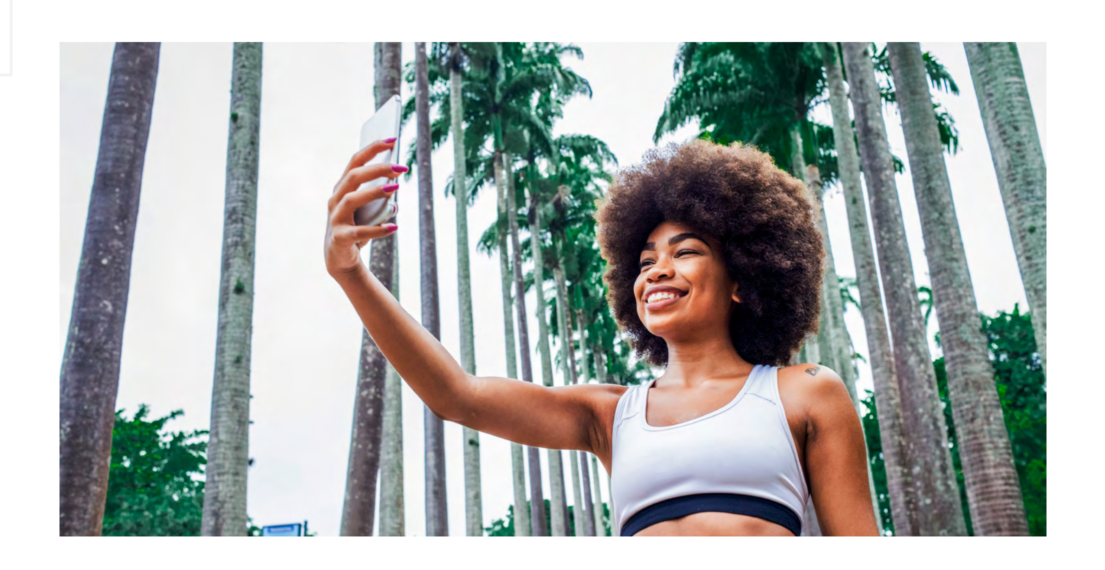
Únicamente Jueces

Solicitudes



1. No hay datos disponibles porque este indicador se contabilizaba como solcitudes atípicas o de bajo volumen.
2. Este dato no es comparable con el resto de años ya que en el 2019 se ha considerado registrar las suspensiones a cuentas a individuales en este indicador (antes se reportaba como bloqueo de contenidos).

Accesos afectados	16.030	Solicitudes rechazadas	N/A



Chile

www.telefonicachile.cl

El Grupo Telefónica en Chile es proveedor de servicios de telecomunicaciones (Banda Ancha, TV digital y Voz), y ha reorganizado su estructura societaria que culminó con el proceso de unificación de las marcas comerciales bajo el nombre de Movistar en octubre de 2009.

Telefónica Chile gestiona más de 10,3 millones de accesos a diciembre de 2019.

Respecto a las cifras financieras, los ingresos de Telefónica en Chile han alcanzado los 1.914 millones de euros y el OIBDA 669 millones de euros.

10.319,9
Accesos totales

Accesos a cierre de 2019 (datos en miles).





Accesos

1.072,9 Telefonía fija	**7.652,0** Telefonía móvil
1.065,6 Datos e Internet	**523,3** TV de pago

Clientes a cierre 2019 (datos en miles).

INTERCEPTACIÓN LEGAL

Contexto legal

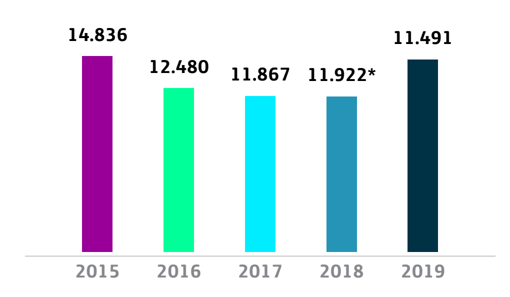
- Código Procesal Penal: Artículos 9, 219, 222 y 223.
- Ley 20.000. Tráfico y control de Estupefacientes.
- Ley 19.913 sobre Lavado de dinero.
- Ley 18.314 que determina consultas terroristas.
- Decreto Ley 211, Artículo 39 letra n).
- Ley 19.974. Ley Sistema Nacional de Inteligencia. Letras a), b), c) y d) de Artículo 24, en relación a los artículos 23 y 28 del mismo cuerpo legal.
- Código Procedimiento Penal. Artículos 177, 113 bis y 113 ter.
- Decreto 142 de 2005 del Ministerio de Transportes y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación.

.

Autoridades Competentes

- Persecutor Penal (Ministerio Público) en virtud de autorización judicial previa.
- Agencias de Inteligencia del Estado, mediante el Sistema Nacional de Inteligencia.
- Policías mediante autorización de Juez Instructor del Crimen (Procedimiento Penal Inquisitivo)
- Fiscalía Nacional Económica, mediante autorización previa de Tribunal de Defensa de Libre Competencia, aprobada por Ministro de Corte de Apelaciones respectivo.

Solicitudes



* El total de 11.922 solicitudes de interceptación legal incluye un total de 714 solicitudes de prorrogas de interceptación legal.

Desglose de Interceptaciones (2019)



Altas	11.020
Prórrogas	471
Bajas	440*

*Las bajas no se consideran dentro del total de solicitudes ya que son bajas que se producen de manera automática por encontrarse en la propia solicitud inicial el plazo para la interceptación.

Accesos afectados	5.590	Solicitudes rechazadas	163

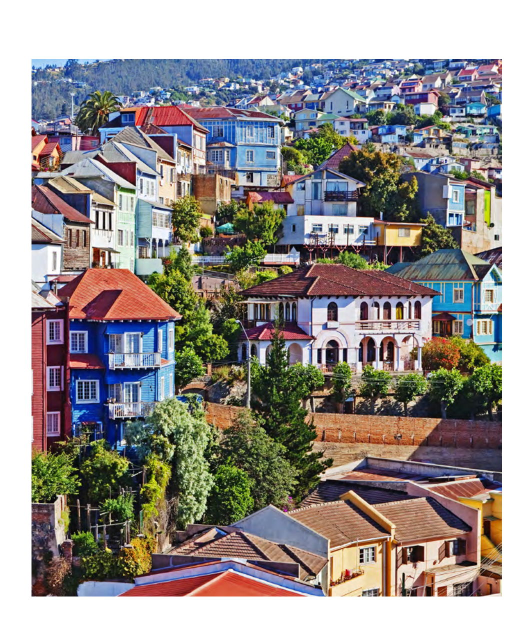
METADATOS ASOCIADOS A LAS COMUNICACIONES

Contexto legal

- La Constitución Política de la República de Chile. A partir de lo dispuesto en el artículo único de la Ley 21.096 que modificó el Artículo 19 número 4 de la Constitución, se asegura a todas las personas: "... la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".
- El Código Procesal Penal: Los Artículos 219 y 222 del Código Procesal Penal, autorizan la entrega de información previa orden del Juez de Garantía, bajo apercibimiento de Desacato en caso de incumplimiento, es decir, bajo la advertencia de incurrir en desobediencia de una resolución judicial; ello de conformidad al Artículo 180 del mismo cuerpo legal y el Artículo 240 del Código Procedimiento Civil.
- El Ministerio Público es la autoridad que dirige la investigación penal y emite órdenes de Investigar que pueden contener requerimientos de información respecto de compañías de telecomunicaciones, ello en conformidad a las disposiciones de los artículos 19 y 180 del Código Procesal Penal . A su vez, y conforme a las disposiciones del artículo 182 del Código Procesal Penal que establecen el secreto de las actuaciones de investigación, el Ministerio Público puede requerir antecedentes de información referidos a la suscripción de servicios contrata-

dos por una determinada persona, remitiendo conjuntamente los datos de identificación del titular o usuario en la respectiva orden de investigar, ello con la finalidad de determinar el grado participación de los eventuales involucrados. Solicita, además, antecedentes de actividad de registros de números IMEI de ciertos dispositivos que son objeto de investigación, información que se remite sin entregar los datos personales de los suscriptores o usuarios asociados a dicho número IMEI.

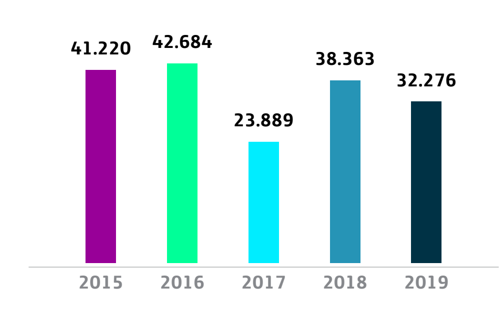
- Ley Orgánica Constitucional del Ministerio Público N°19.640.
- Procedimiento penal inquisitivo: Artículo 120 bis y 171 del Código de Procedimiento Penal.



Autoridades Competentes

- Persecutor Penal Público: Ministerio Público.
- Policías con autorización del ministerio Público y orden de investigar.
- Juez de Sumario en Procedimiento penal inquisitivo. (Código Procedimiento Penal)
- Agencias de Inteligencia de Estado con autorización judicial previa.

Solicitudes



Accesos afectados	10.357
Solicitudes rechazadas	675

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

- Ley 17.336, sobre Propiedad Intelectual. Artículo 85 Q, en relación a lo dispuesto en el Artículo 85 R letras a) y b) del mismo cuerpo legal.
- Código de Procedimiento Civil: Medidas precautorias o cautelares innominadas.
- Código Procesal Penal: Medidas precautorias o cautelares innominadas.

Autoridades Competentes

- Tribunales ordinarios y especiales dependientes orgánicamente del Poder Judicial.
- Tribunal de Defensa de la Libre Competencia, sujeto a la superintendencia directiva, correccional y económica de la Corte Suprema, que estén conociendo de un proceso contencioso.

Solicitudes

2015	2016	2017	2018	2019
1	0	0	1[1]	0

1. Por violación de derechos de autor (Ley 17.336 de Propiedad Intelectual).

URL afectadas	0
Solicitudes rechazadas	0

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio

Autoridades Competentes

No aplica.

Solicitudes

2015	2016	2017	2018	2019
N/A	N/A	N/A	N/A	N/A

Accesos afectados	N/A
Solicitudes rechazadas	N/A



Colombia

www.telefonica.co

Telefónica tiene presencia en Colombia desde el año 2004. Comenzó con actividades en el mercado móvil, tras la adquisición de la operación celular de Bellsouth en el país. Posteriormente, en el año 2006, Telefónica adquirió el control y la gestión de Colombia Telecom. Telefónica proporciona hoy en el país servicios de telecomunicaciones de voz, banda ancha y televisión de pago.

Telefónica Colombia gestiona mas de 19,2 millones de accesos a cierre de 2019.

Los ingresos de Telefónica en Colombia alcanzaron 1.410 millones de euros y el OIBDA sumó 558 millones de euros.



Accesos a cierre de 2019 (datos en miles).



Accesos

1.487,7 Telefonía fija

16.080,4 Telefonía móvil

1.179,2 Datos e Internet

528,1 TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

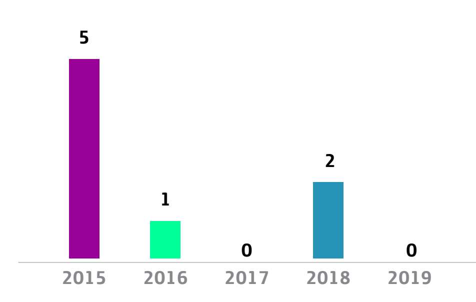
Contexto legal

- Constitución Colombiana: Artículo 15 y Artículo 250.
- Ley 906. Código Procedimiento Criminal de 200. Art. 235. Modificado por el artículo 52 de la Ley 1453 de 2011.
- Ley 1621 de 2013. Art. 44.
- Decreto 1704 de 2012. Artículo 1-8.
- Decreto 2044 de 2013. Art. 3.

Autoridades Competentes

- Fiscalía General de la Nación.
- A través del grupo de Policía Judicial designado para la investigación del caso.

Solicitudes*



*Solicitudes sobre líneas fijas

Líneas moviles: No se reportan interceptaciones sobre líneas móviles: La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa sobre las líneas móviles.

Accesos afectados	0	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

Contexto legal

- Constitución Colombiana: Artículo 250.
- Ley 906 de 2004. Art. 235.
- Ley 1621 de 2013. Ar. 44.
- Decreto 1704 de 2012. Art. 1-8.

Autoridades Competentes

- Autoridades con funciones de policía judicial, y pueden ser de orden permanente o transitorio:

  El artículo 312 del nuevo código de procedimiento penal, define que las entidades que poseen facultades permanentes de Policía Judicial son las siguientes:

  - Fiscalía General de la Nación y todos sus servidores públicos que desempeñen funciones judiciales (Art. 249 CN y Art. 112, 113 CPP).
  - Policía Judicial: C.T.I., Policía Nacional y D.A.S., facultados por comisión de autoridad judicial competente y por mandato legal (Art. 311 a 320 CPP).
  - Grupos de Acción Unificado "Antisecuestro y Extorsión" (Ley 282 de 1996).

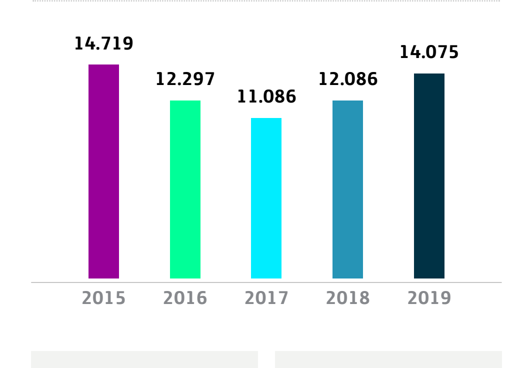
Ejercen funciones especiales de policía judicial, en asuntos de su competencia:

- Contraloría General de la Nación (Art. 267 CN y Art. 312 CPP).
- Procuraduría General de la Nación (Art. 275 CN y Art. 312 CPP).
- Dirección Nacional de Impuestos y Aduanas Nacionales _ DIAN (ver numeral 2, Capitulo II).
- Entidades públicas que ejerzan funciones de vigilancia y control (MINTIC, ANE, SIC y CRC).
- Los alcaldes e inspectores de policía, en los lugares del territorio donde no hubiere miembros de la policía judicial de la Policía Nacional.
- Directores Nacional y regional del INPEC, los directores de los establecimientos de reclusión y el personal de custodia y vigilancia, conforme a lo señalado en el Código Penitenciario y Carcelario.
- Inspecciones de Policía (Art. 312 CPP).



- Para investigaciones de índole disciplinarias (la Ley 734 de 2002 (código único Disciplinario) están facultados las oficinas de control disciplinario interno.
- Policías con autorización del ministerio Público y orden de investigar.
- Juez de Sumario en Procedimiento penal inquisitivo. (Código Procedimiento Penal).
- Agencias de Inteligencia de Estado con autorización judicial previa.

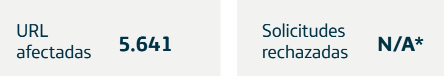
Solicitudes



Accesos afectados	42.225	Solicitudes rechazadas	140

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

TOTAL URL AFECTADAS



URL afectadas	5.641	Solicitudes rechazadas	N/A*

*N/A por el sistema de bloqueo establecido por ley.

Material de abuso sexual infantil

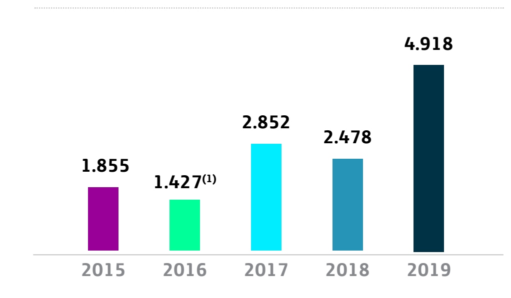
Contexto legal

- Ley 679 de 2001: Artículos 7 y 8.
- Decreto 1524 de 2002: Artículos 5 y 6.
- Ley 1450 de 2011: Artículo 56.
- Resolución CRC 3502 de 2011.

Autoridades Competentes

- La Policía Nacional le envía al Ministerio de las Tecnologías de la Información y las Comunicaciones un listado de URLs con orden de bloqueo para que el Ministerio lo publique en su página web y pueda ser consultado por los PSI. Para acceder a este listado, los PSI deben contar con un usuario y una contraseña que es suministrada previamente por el Ministerio, para evitar que cualquier persona pueda consultar los URLs que tienen orden de bloqueo por contener material de pornografía infantil.

Nº URL*



(1)Desde septiembre de 2016 entró en operación la plataforma "WOLF Control de Contenidos" la cual filtra de manera especializada todo el contenido ilegal tipificado por las autoridades locales como pornografia infantil.

El listado se continua actualizando y publicando de manera periodica por medio de la página web del Ministerio de las Tecnologías de la Información y las Comunicaciones.

* Número de URLs agregados al listado publicado por MinTIC durante ese año.

Juegos Ilegales

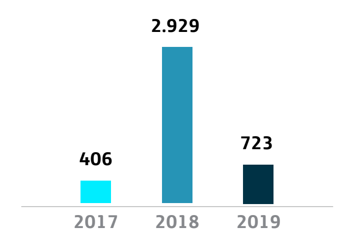
Contexto legal

- Ley 1753 de 2015: Artículo 93, parrágrafo 3.
- Ley 1450 de 2011: Artículo 56.
- Resolución CRC 3502 de 2011.

Autoridades Competentes

Coljuegos, empresa industrial y comercial del Estado encargada de la administración del monopolio rentistico de los juegos de suerte y azar, en conjunto con la Policia Nacional identifican portales Web en los que se comercializan juegos de suerte y azar no autorizados y le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI el listado de las URLs que deben bloquear.

Nº URL





Orden judicial

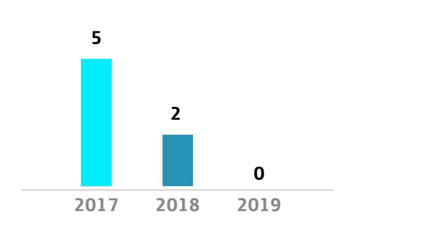
Contexto legal

- Ley 1273 de 2009: Artículo 269F.
- Ley 1340 de 2009: Artículo 18.
- Ley 1450 de 2011: Artículo 56.
- Resolución CRC 3502 de 2011.

Autoridades Competentes

La Fiscalia General de la Nación y la Superintendencia de Industría y Comercio dentro de las investigaciones que adelantan le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI las URLs que deben bloquear.

Nº URL



SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

Ley 1341 de 2009. Art. 8. Casos de emergencia, conmoción o calamidad y prevención.

Decreto 2434 de 2015, Resolución CRC 4972 de 2016 – Obliga a priorizar las llamadas entre autoridades para atender emergencias. Esta priorización implica terminar llamadas de usuarios que no están en el listado de números.

Autoridades Competentes

Se darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.

Solicitudes

2015	2016	2017	2018	2019
0	0	0	0	0

Accesos afectados **0**

Solicitudes rechazadas **0**

Ecuador

www.telefonica.com.ec

En Ecuador, Telefónica inició sus operaciones en el 2004, con la adquisición de la operación móvil de BellSouth en el país (que en ese momento era el segundo operador ecuatoriano, con 816.000 clientes y una cuota del 35% del mercado).

La compañía está en 24 provincias del país y comunica a más de 5 millones de ecuatorianos con servicios móviles, generando una red de productividad que beneficia directa e indirectamente a más de 100.000 familias del Ecuador.

Telefónica gestiona 4.393 millones de accesos en Ecuador a cierre de 2019.

Los ingresos ascendieron a 484 millones de euros y el OIBDA a 193 millones de euros.



Accesos a cierre de 2019 (datos en miles).



Accesos

0,0 Telefonía fija	4.393 Telefonía móvil
0,0 Datos e Internet	0,0 TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

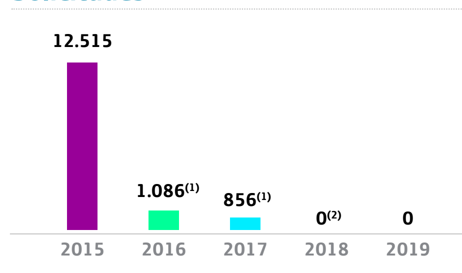
Contexto legal

- Código Orgánico Integral Penal (Art. 476-477).
- Contrato de Concesión suscrito entre OTECEL S.A. y el Estado Ecuatoriano.

Autoridades Competentes

Fiscal competente dentro de una investigación.

Solicitudes



(1) Debido a un cambio de normativa ahora la fiscalía responde directamente sobre los pedidos de intervención y de datos en materia penal. Telefónica solo recibe ya en materia civil.

(2) El Estado Ecuatoriano a través de la Fiscalía General de la Nación ordenó que este tipo de procesos se realice desde el año 2018 sin la intervención de la operadora. Es decir, es la Fiscalía la única entidad autorizada a realizar este tipo de intercepción en tiempo real.

Accesos afectados	0	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

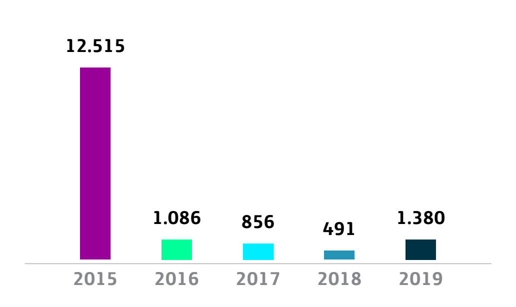
Contexto legal

- Código Orgánico Integral Penal. Artículo 499

Autoridades Competentes

- Jueces de Garantías Penales.

Solicitudes



Accesos afectados	1.320	Solicitudes rechazadas	0



BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

- Código Orgánico Integral Penal. Art. 583.
- Código Orgánico de la Economía Social de los Conocimientos. Art. 563 y 565.

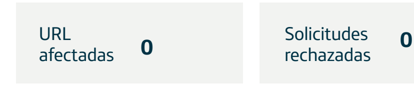
Autoridades Competentes

- El Fiscal puede solicitar de manera fundamentada a Juez de Garantías penales autorización para proceder.
- SENADI (Servicio Nacional de Derechos Intelectuales puede ordenar medidas cautelares).

Solicitudes

2015	2016	2017	2018	2019
0	0	0	1*	0

*Por vulnerar derechos de propiedad intelectual



URL afectadas	Solicitudes rechazadas
0	0

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

CONSTITUCIÓN DEL ECUADOR. Art. 164y 165

Autoridades Competentes

Aquella(s) que el Presidente de la República delegue en su nombre según las circunstancias que refleja la ley.

Solicitudes

2015	2016	2017	2018	2019
0	0	0	0	0

Accesos afectados	Solicitudes rechazadas
0	0



España

www.telefonica.es

Telefónica desarrolla su actividad en España, principalmente en los negocios de telefonía fija y móvil, con la banda ancha como herramienta clave para el desarrollo de ambos, y en los servicios de TI y soluciones. Telefónica España es la compañía de telecomunicaciones líder en España por accesos, incluyendo voz, datos, televisión y acceso a internet y ofrece a sus clientes los más innovadores servicios y las tecnologías más punteras para conseguir el objetivo de convertirse en la primera telco digital.

Telefónica España gestiona más de 41.8 millones de accesos a cierre de 2019.

Los ingresos por operaciones totalizaron 12.767 millones de euros y el OIBDA alcanzó los 3.687 millones de euros en 2019.

41.837,7
Accesos totales

Accesos a cierre de 2019 (datos en miles).





Accesos

9.024,1
Telefonía fija

18.916,9
Telefonía móvil

6.034,8
Datos e Internet

4.073,8
TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

Contexto legal

- Constitución Española (art. 18).
- Ley de enjuiciamiento Criminal (Artículo 588.)
- Ley 9/2014, General de Telecomunicaciones (Art. 39 y 42). Además, esta ley ha sido modificada en virtud de lo establecido en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Así existe una nueva redacción al apartado 6 del artículo 4 y al apartado 1 del artículo 81.
  - Apartado 6 del artículo 4, " El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de los correspondientes servicios o de la explotación de las correspondientes redes.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final."

  - Apartado 1 del artículo 81, "Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Economía y Empresa, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) Cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

b) Cuando exista una amenaza inmediata y grave para la salud pública.

c) Cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias.

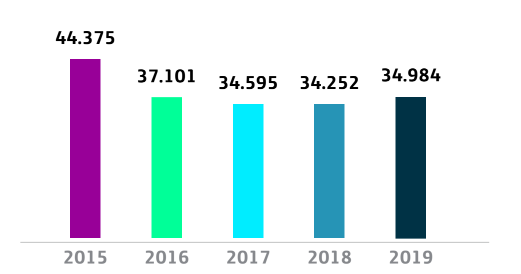
d) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

e) Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.»

Autoridades Competentes

- Jueces de los Juzgados de Instrucción
- Casos excepcionales (urgencia, bandas armadas) el Ministro del Interior o el Secretario de Estado de Seguridad. En 24 horas el juez ratificará o revocará la solicitud
- El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional.

Solicitudes



Desglose de Interceptaciones (2019)



Altas	12.944
Prórrogas	15.700
Bajas	6.340
Accesos afectados	14.215
Solicitudes rechazadas	5.374






METADATOS ASOCIADOS A LAS COMUNICACIONES

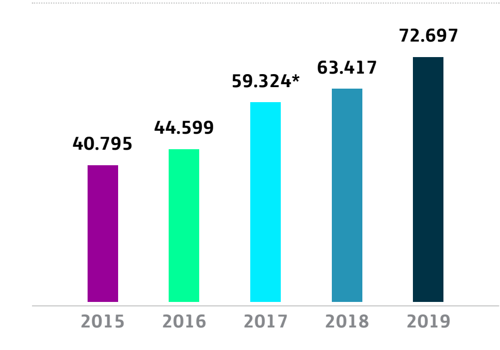
Contexto legal

- Ley 25/2007 de Conservación de Datos. (Artículos 1-10).
- Ley 9/14, General de Telecomunicaciones (Artículos 39-42).

Autoridades Competentes

- Juzgados.
- Policía Judicial y Ministerio Fiscal (Ley Orgánica 13/2015 de modificación de la Ley de Enjuicia-miento Criminal).

Solicitudes



* En el año 2017 se puso en marcha un nuevo sistema de envío de mandamientos judiciales por parte de las Fuerzas y Cuerpos de Seguridad del Estado, en el que cada petición de datos da lugar a un requerimiento individual. Con el sistema anterior, que aún está en funcionamiento para la mayoría de estos agentes, un mismo mandamiento judicial podía dar lugar a múltiples Solicitudes de datos, aunque se contabilizara como una sola.

Accesos afectados	No disponible*	Solicitudes rechazadas	12.397

* La naturaleza de ciertos requerimientos y la configuración de las herramientas no permiten aportar este dato.

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

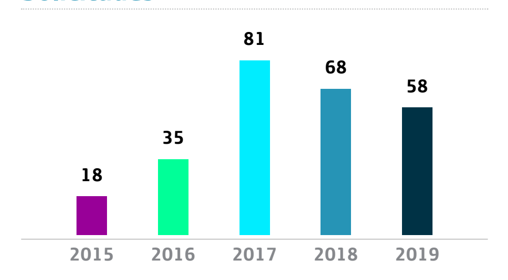
Contexto legal

- Real Decreto 1889/2011, de 30 de diciem-bre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual. (Artículo 22 y 23).
- Texto Refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril (Artículo 138).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (Artículo 8).

Autoridades Competentes

- Comisión Nacional de los Mercados y de la Competencia.
- Juzgados Mercantiles/Civiles/Cont.-Adminis-trativo/Penal.
- Comisión Nacional de la Propiedad Intelectual.
- Dirección General del Juego.
- Agencia del Medicamento/Dopaje/Salud/ Deporte.

Solicitudes



Propiedad intelectual

Nº solitudes	29	Nº de URL afectadas	770

Delitos

Nº solitudes	24	Nº de URL afectadas	131

Medicamentos

Nº solitudes	2	Nº de URL afectadas	2

Juego ilegal

Nº solitudes	3	Nº de URL afectadas	1.385

URL afectadas	2.288*	Solicitudes rechazadas	0

*Incluye URL y direcciones IP



SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

Autoridades Competentes

No aplica.

Solicitudes

2015	2016	2017	2018	2019
N/A	N/A	N/A	N/A	N/A

Accesos afectados	N/A
Solicitudes rechazadas	N/A

México

www.telefonica.com.mx

Telefónica México participa y compite en el mercado de las telecomunicaciones desde 2001 e impulsa el desarrollo de las telecomunicaciones en el país. Hoy cuenta con la mejor cobertura nacional, con más de 93 mil localidades, 90 mil kilómetros carreteros y más de 25.2 millones de clientes.

Las ofertas comerciales se encuentran disponibles en 231 Centros de Atención a Clientes (CAC), 36 Plazas Movistar y 26 'Smart Stores' o Tiendas Inteligentes a nivel nacional, 3 Centros de Experiencia Movistar y más de siete mil puntos de venta indirecta en todo el país.

Telefónica en Mexico gestiona más de 26.6 millones de accesos a cierre de 2019.

Respecto a las cifras financieras, los ingresos de Telefónica en Mexico alcanzaron 1.244 millones de euros y el OIBDA[1] fue de 147 millones de euros.

[1] Incluye el impacto por -239M€ (octubre-diciembre 2019) consecuencia de la transformación del modelo operacional de T. México tras el acuerdo alcanzado con AT&T.



26.088,3
Accesos totales

Accesos a cierre de 2019 (datos en miles).





Accesos

0,0 Telefonía fija	**26.088,3** Telefonía móvil
0,0 Datos e Internet	**0,0** TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

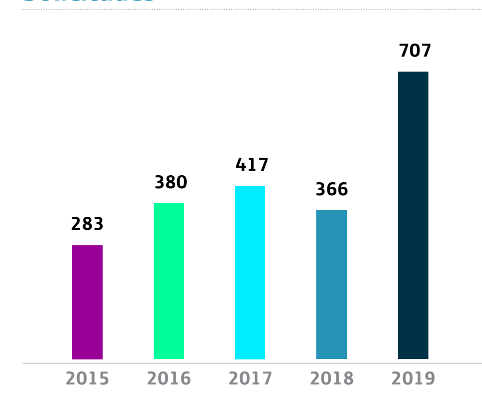
Contexto legal

- Constitución Política de los Estados Unidos Mexicanos (artículo 16, párrafo 12).
- Código Nacional de Procedimientos Penales, artículo 291.
- Ley Federal Contra la Delincuencia Organizada, artículo 16.

Autoridades Competentes

La autoridad judicial federal es quien determina si es procedente la solicitud de la autoridad investigadora respecto a la intervención de comunicaciones, quien ordena al concesionario establecer la medida por un tiempo determinado.

Solicitudes



Desglose de Interceptaciones (2019)

Altas	368
Prórrogas	10
Bajas	329

Accesos afectados	460	Solicitudes rechazadas	2

METADATOS ASOCIADOS A LAS COMUNICACIONES

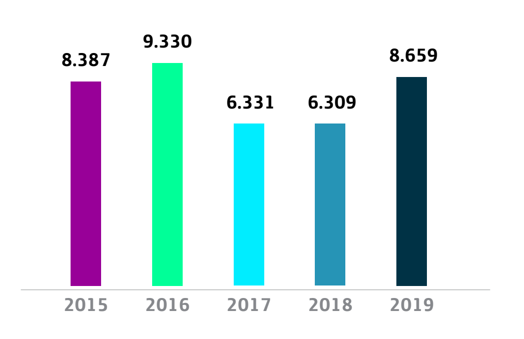
Contexto legal

- Ley Federal de Telecomunicaciones y Radiodifusión (articulo 190).
- Código Nacional de Procedimientos Penales (artículo 303).
- Ley de Vías Generales de Comunicaciones (artículo 122).

Autoridades Competentes

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Solicitudes



Accesos afectados	18.331	Solicitudes rechazadas	149

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

No existen leyes en el marco regulatorio que permitan bloqueo y restricción de contenidos.

Autoridades Competentes

No aplica

Solicitudes

2015	2016	2017	2018	2019
N/A	N/A	N/A	N/A	N/A

URL afectadas	N/A
Solicitudes rechazadas	N/A

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

Autoridades Competentes

No aplica

Solicitudes

2015	2016	2017	2018	2019
N/A	N/A	N/A	N/A	N/A

Accesos afectados	N/A
Solicitudes rechazadas	N/A

Perú

www.telefonica.com.pe

Telefónica comenzó a operar en el mercado peruano a mediados de la década de los 90. Telefónica en Perú gestiona más de 17,6 millones de accesos en diciembre de 2019.

Respecto a las cifras financieras, los ingresos de Telefónica en Perú alcanzaron 2.102 millones de euros y el OIBDA sumó 354 millones de euros.



17.640,6
Accesos totales

Accesos a cierre de 2019 (datos en miles).



Accesos

2.247 Telefonía fija	**11.897,4** Telefonía móvil
1.991,5 Datos e Internet	**1.505,0** TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

Contexto legal

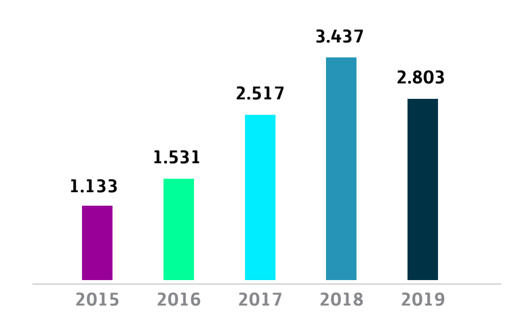
- Constitución Política del Perú (Artículo 2° inciso 10).
- Ley de Telecomunicaciones (Decreto Supremo N° 013-93-TCC – Artículo 4°) y su Reglamento (Decreto Supremo N° 020-2007-MTC – Artículo 13°).
- Ley N° 27697: Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.
- Decreto Legislativo N° 1182.

En todos los contratos de concesión existe la cláusula referida al secreto de las telecomunicaciones y protección de datos personales que establece que la empresa salvaguardará los mismos y mantendrá la confidencialidad de la información personal relativa a sus clientes, salvo que exista una orden judicial específica.

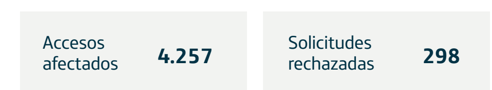
Autoridades Competentes

- Juez (Poder Judicial).
- Fiscal de la Nación, Fiscales Penales y Procuradores Públicos (Ministerio Público) con autorización del Juez.

Solicitudes*



*Se incluyen altas, prorrogas y cese de interceptaciones.



METADATOS ASOCIADOS A LAS COMUNICACIONES

Contexto legal

- Constitución Política del Perú (Artículo 2° inciso 10).
- Ley de Telecomunicaciones (Decreto Supremo N° 013-93-TCC – Artículo 4°) y su Reglamento (Decreto Supremo N° 020-2007-MTC – Artículo 13°).
- Ley N° 27697: Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.
- Decreto Legislativo N° 1182 que regula el uso de las Telecomunicaciones para la Identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

En todos los contratos de concesión existe la cláusula referida al secreto de las telecomunicaciones y protección de datos personales que establece que la empresa salvaguardará los mismos y mantendrá la confidencialidad de la información personal relativa a sus clientes, salvo que exista una orden judicial específica.

Autoridades Competentes

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Solicitudes







BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

Ley de Derechos de Autor

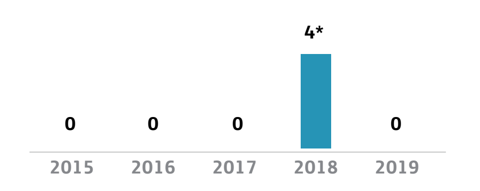
Autoridades Competentes

- INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual)

En estricto, no ha habido un cambio legislativo, no existe alguna autoridad que pueda bloquear contenidos web, salvo el Poder Judicial. Sin embargo, existe una excepción en el caso de INDECOPI. Y es que, en virtud del artículo 169 de la Ley de Derechos de Autor, la Comisión de Derechos de Autor del INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual) tiene competencia para dictar medidas preventivas o cautelares y sancionar de oficio a solicitud de parte, las infracciones o violaciones a la legislación nacional de derechos de autor y derechos conexos; pudiendo amonestar, incautar, decomisar, disponer el cierre temporal o definitivo de los establecimientos donde se cometa la infracción.

Para el Indecopi, en la medida que a través de los sitios web se estaría realizando actos que vulneran el derecho de comunicación pública de las empresas denunciantes, la administración puede ordenar el bloqueo del acceso en territorio peruano al sitio web infractor, mediante el bloqueo basado en DNS y el bloqueo basado en URL.

Solicitudes



*Requerimientos de INDECOPI (medidas cautelares en casos por propiedad intelectual).

URL afectadas	Solicitudes rechazadas
0	0

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

Reglamento de la Ley de Telecomunicaciones (D.S. N° 020-2007-MTC - Artículos 18° y 19°)

En los contratos de concesión se prevé que en caso de emergencia, crisis y seguridad nacional la empresa concesionaria brindará los servicios de telecomunicaciones priorizando las acciones de apoyo al Estado y siguiendo las instrucciones del MTC.

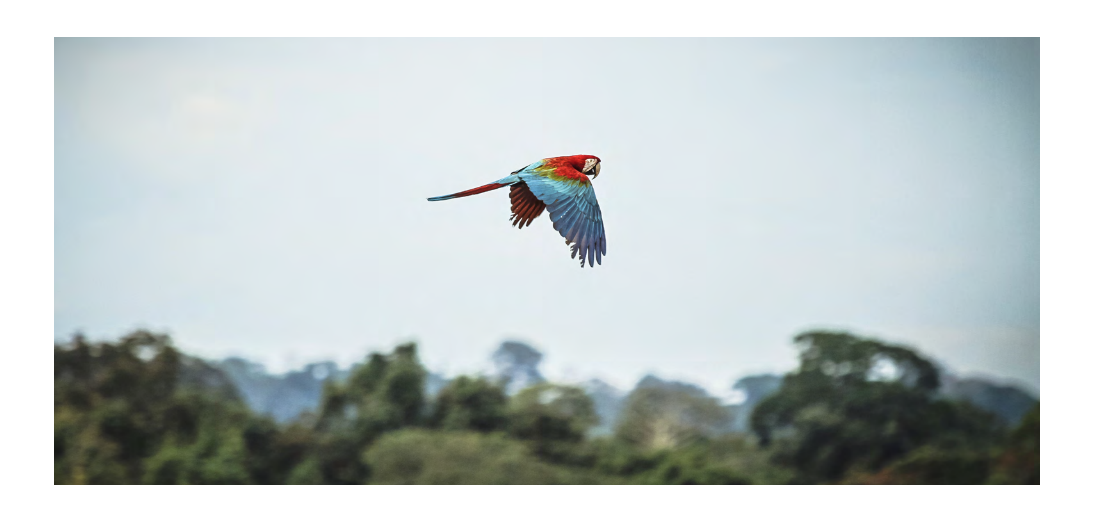
Autoridades Competentes

- Ministerio de Transportes y Comunicaciones (MTC).
- Sistema de Defensa Nacional y Civil.

Solicitudes

2015	2016	2017	2018	2019
0	0	0	0	0

Accesos afectados	Solicitudes rechazadas
0	0





Reino Unido

www.telefonica.com/en

Telefónica comienza a operar en el Reino Unido a principios del 2006 tras adquirir O2, que se convierte en la marca comercial de Telefónica UK Limited.

La compañía ofrece un amplio abanico de productos y servicios de telefonía móvil sobre sus redes 2G, 3G y 4G. Además, O2 es propietaria de 50% de Tesco Mobile, así como de O2-Wifi, que cuenta con más de 6 millones de clientes activos. O2 cuenta con una cadena de más de 450 tiendas.

Telefónica cuenta con más de 34,8 millones de accesos en Reino Unido a cierre de 2019.

Respecto a las cifras financieras, Los ingresos totales se sitúan en 7.109 millones de euros y el OIBDA en 2.144 millones de euros.





Accesos a cierre de 2019 (datos en miles).



Accesos

313,3 Telefonía fija	**25.803,3** Telefonía móvil
28,9 Datos e Internet	**0,0** TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

Contexto legal

La interceptación legal se rige por la Ley de poderes de investigación de 2016 (IPA). La Comisión de Poderes Investigadores (IPC) y la Oficina de la Comisión de Poderes Investigadores (IPCO) están ahora plenamente establecidos. La IPCO supervisa la aplicación y el cumplimiento de las solicitudes de interceptación legal presentadas con arreglo a la Ley de facultades de investigación.

Autoridades Competentes

En virtud de la IPA, la Secretaría de Estado del departamento gubernamental pertinente puede emitir una orden de interceptación en los casos en que la misma Secretaría del Estado considere que es necesaria para la seguridad nacional, para prevenir o detectar delitos graves o para salvaguardar el bienestar de la economía del Reino Unido.

Actualmente, en el Reino Unido hay ocho agencias autorizadas que pueden solicitar la emisión de una orden por parte de la Secretaría de Estado. Son:

- una persona que es jefe de un servicio de inteligencia;
- el Director General de la Agencia nacional contra la delincuencia;
- el Comisario de la Policía municipal;
- el Jefe de policía del Servicio de Policía de Irlanda del Norte;
- el Jefe de Policía del Servicio de Policía de Escocia;
- los comisionados de la Agencia Tributaria y de Aduanas de Su Majestad;
- el Jefe de Inteligencia para la Defensa; y
- una persona que es la autoridad competente de un país o territorio fuera del Reino Unido a los efectos de un dispositivo de asistencia mutua de la UE o de un acuerdo internacional de asistencia mutua.

Para obtener una orden de interceptación legal, la autoridad solicitante debe enviar una solicitud al correspondiente Secretario de Estado. El Secretario de Estado debe considerar, para decidir si emite la orden, si (entre otras cosas) existen fundamentos para justificar la emisión de la orden (ver más arriba) y si la interceptación autorizada por la orden es proporcionada a lo que se busca conseguir con dicha interceptación.

A partir de noviembre de 2018, todas las solicitudes de interceptación legal se han realizado de conformidad con la Ley de Protección de la Propiedad Intelectual y deben ser autorizadas por el Secretario de Estado (o su adjunto) en forma de una orden judicial y un juez. El juez considerará los mismos factores que el Secretario de Estado (es decir, si hay motivos para emitir la orden y si la conducta es proporcional al objetivo).

Solicitudes*

N/D	N/D	N/D	N/D	N/D
2015	2016	2017	2018	2019

*El artículo 57 de la Ley de Prevención del Terrorismo prohíbe la divulgación de la existencia de cualquier orden de interceptación legal, salvo en circunstancias excepcionales, según el artículo 58 de la Ley de Prevención del Terrorismo.

La OIPC elabora un informe anual sobre la adquisición y divulgación de datos de comunicaciones por parte de los organismos de inteligencia, las fuerzas de policía y otras autoridades públicas. En él se dan detalles de las cifras globales, pero no por empresa. Véase: https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190321.pdf

Accesos afectados	N/D	Solicitudes rechazadas	N/D



METADATOS ASOCIADOS A LAS COMUNICACIONES

Contexto legal

Las disposiciones para la divulgación de datos de comunicación en virtud de la RIPA y la ISA y la Ley de 2015 sobre lucha contra el terrorismo y de seguridad (CTSA) fueron reemplazadas por la IPA en cuanto se haya establecido la IPCO y esté plenamente operativa. Hasta entonces, son vigentes las disposiciones actuales.

La disposición para la retención de datos, previamente almacenados en virtud de la Ley de 2014 sobre conservación de datos y facultades de investigación (DRIPA) se realiza ahora mediante una notificación de retención emitida en virtud de la IPA.

Autoridades Competentes

Marco de la RIPA

- Según el apartado 22 (4) de la RIPA una persona con un cargo, rango o posición prescrito, en una autoridad pública destacada, designado con el poder de adquirir datos de comunicación por orden en virtud del apartado 25 (2) y en virtud de la Orden de regulación de las facultades de investigación (Datos de Comunicación) 2010 (SI 2010/480) podría emitir una notificación. Las personas que pueden emitir una notificación son altos cargos policiales u otros altos cargos en los servicios de seguridad pertinentes.
- En virtud del apartado 22 (3) de la RIPA, las personas dentro de una autoridad pública pueden recibir autorización para la obtención directa de datos de comunicación en el contexto de ciertas circunstancias.

Régimen de IPA

- En virtud del apartado 61 de la IPA, un alto cargo designado de la autoridad pública pertinente puede emitir una autorización para divulgar datos. Igual que en virtud de la RIPA, en virtud de la IPA las personas que pueden autorizar la divulgación de datos son altos cargos policiales u otros altos cargos en los correspondientes servicios de seguridad.

Solicitudes*

2015	2016	2017	2018	2019
N/D	N/D	N/D	N/D	N/D

*El apartado 82 de la IPA tipifica como delito la divulgación de detalles de solicitudes de datos de comunicación.

La IOCCO emite un informe anual en el que se presentan las cifras totales del sector. Los números individuales de la empresa no se desglosan. Esta práctica continuará con la Comisión sobre las facultades de investigación.

Accesos afectados	N/D	Solicitudes rechazadas	N/D

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

Contexto legal

- Apartado 97A de la Ley de 1988 sobre derechos de autor, diseños y patentes.
- Artículo 37, apartado 1, de la Supreme Courts Act 1981 (Ley de 1981 del Tribunal Supremo).
- Artículo 11 de la Directiva sobre la Protección de la Propiedad Intelectual.

El único filtro de contenidos que el gobierno británico exige a los operadores de banda ancha y móviles del Reino Unido es el uso de la lista de bloqueo de la Internet Watch Foundation (IWF) para los sitios ilegales de abuso infantil. Esto es parte de un acuerdo entre los CSP (Políticas de Seguridad de Contenido) y los cuerpos policiales para prevenir la explotación infantil. Se trata de un código de práctica voluntario y no de un requerimiento legal. En 2004, Telefónica Reino Unido fue uno de los signatarios fundadores del código de prácticas de protección de la infancia de los operadores móviles del Reino Unido para la autorregulación de nuevas formas de contenido en los móviles. Este código también explica que voluntariamente bloquearemos el acceso a contenidos clasificados como de 18 años a menos que un cliente haya confirmado que es mayor de 18 años. Se trata de contenido legal, las páginas legales para adultos (se excluyen las páginas ilegales de abuso a menores que detecta la IWF).

Este código también explica que bloquearemos voluntariamente el acceso a los contenidos limitados a mayores de 18 años, excepto en el caso que el cliente haya confirmado que es mayor de edad. Se entiende por contenido legal.

Autoridades Competentes

- Internet Watch Foundation
- Tribunales

Solicitudes*

2015	2016	2017	2018	2019
N/D	N/D	N/D	N/D	N/D

*Solo la IWF, las estadísticas no están disponibles

URL afectadas	N/D	Solicitudes rechazadas	N/D



SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

Telefónica UK está obligada a limitar el servicio en situaciones de sobrecarga de la red (por ejemplo en grandes catástrofes, etc.) para priorizar los servicios de respuesta a emergencias. El esquema de acceso preferente de telecomunicaciones móviles (MTPAS) se creó bajo la Ley de 2004 sobre contingencias civiles (CCA). La elegibilidad está restringida a las organizaciones que tienen un papel para responder a, o recuperarse de, una emergencia tal como se define en la CCA.

Al inicio de una respuesta a una emergencia, el jefe de policía pertinente seguirá el protocolo acordado para notificar a todos los operadores de red móvil que se ha producido un incidente grave y solicitar la monitorización de los niveles de tráfico de llamadas. Si la red se congestiona, se solicitará a los operadores de red que consideren la posibilidad de acogerse a la MTPAS para facilitar que los equipos de emergencia realicen llamadas con prioridad sobre otros clientes.

Autoridades Competentes

- El jefe de policía pertinente seguirá el protocolo acordado.
- La suspensión del servicio se negocia entre las autoridades de emergencias y los CSP, y Telefónica UK puede oponerse si cree que la acción no impactaría la carga de red.

Solicitudes*

2015	2016	2017	2018	2019
0	0	0	0	0

Accesos afectados	0
Solicitudes rechazadas	0

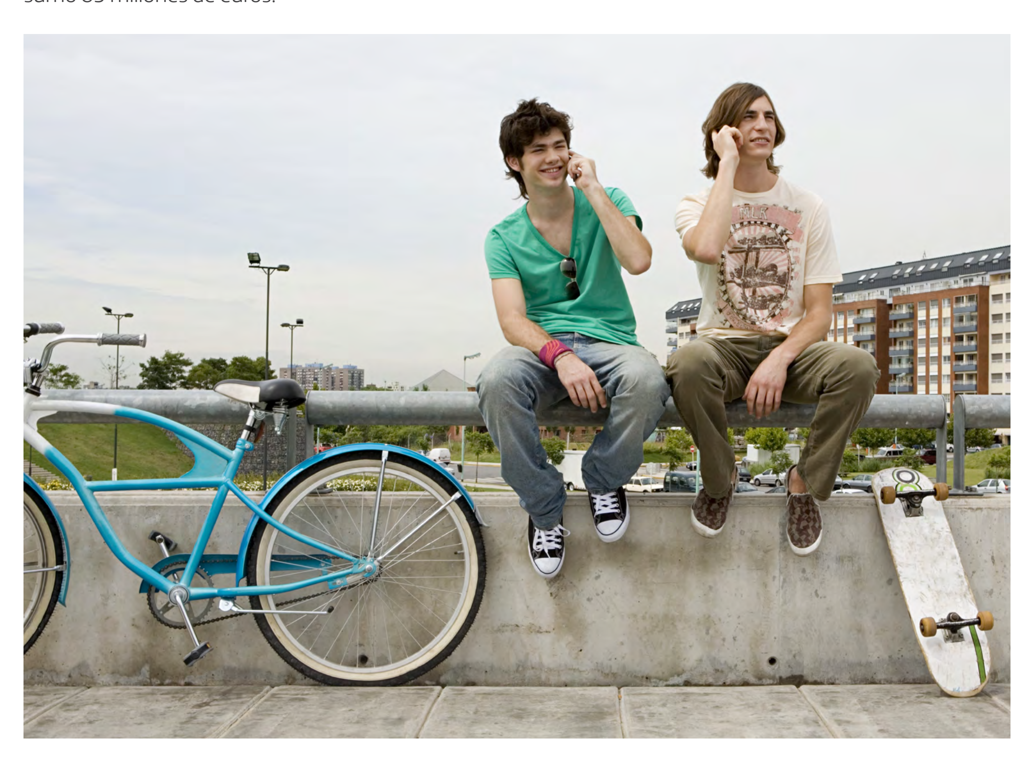


Uruguay

www.movistar.com.uy

Telefónica está presente en Uruguay desde 2005.

En 2019 Los ingresos de Telefónica en Uruguay alcanzaron los 219 millones de euros y el OIBDA sumó 83 millones de euros.



1.676,1
Accesos totales

Accesos a cierre de 2019 (datos en miles).

Accesos

0,0 Telefonía fija	**1.676,1** Telefonía móvil
0,0 Datos e Internet	**0,0** TV de pago

Accesos a cierre de 2019 (datos en miles).

INTERCEPTACIÓN LEGAL

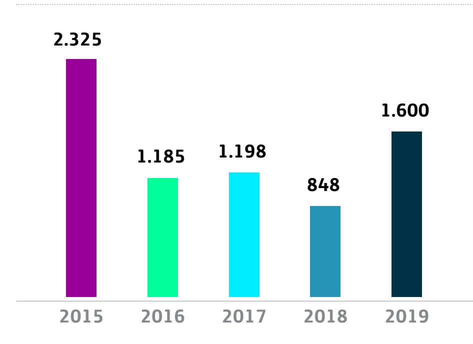
Contexto legal

- Constitución de la República (art. 28).
- Ley 18.494 (Art.5).
- Decreto reservado de fecha 13 de marzo de 2014.

Autoridades Competentes

- Jueces penales a cargo de una investigación, previa solicitud del Ministerio Público y a través de la UNATEC (órgano del Ministerio del Interior encargado de centralizar dichas solicitudes).

Solicitudes



Desglose de Interceptaciones (2019)



Altas	867
Prórrogas	489
Bajas	244

Accesos afectados	867
Solicitudes rechazadas	22

METADATOS ASOCIADOS A LAS COMUNICACIONES

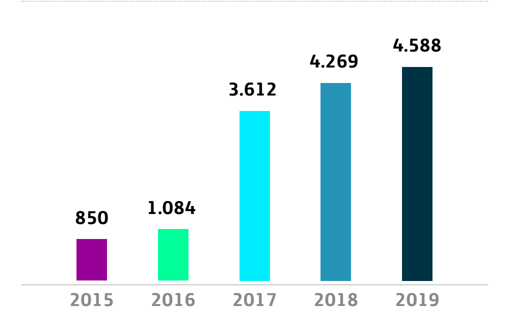
Contexto legal

- Constitución de la República (Art. 28).
- Ley 18.494 (artículo 5).
- Decreto reservado de fecha 13 de marzo de 2014.

Autoridades Competentes

- Jueces, mediante solicitud escrita y fundada.

Solicitudes*



* El incremento respecto al 2016 se corresponde porque a partir de 2017 se cuenta con una herramienta que permite contabilizar los requerimientos por cada cliente afectado. Hasta entonces un mismo requerimiento (oficio judicial) contenía más de un cliente afectado. A partir del 2017 cada requerimiento se corresponde a un cliente afectado. Por tanto, se debe al cambio en el criterio de contabilización.

Accesos afectados	4.588
Solicitudes rechazadas	36



BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

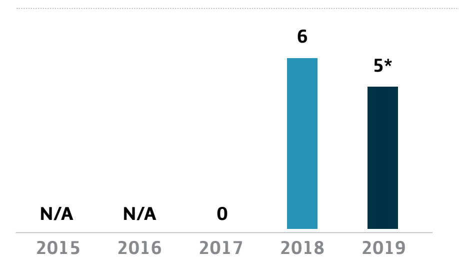
Contexto legal

- Ley 19.535 del 25 de septiembre de 2017 (artículos 244 y 245).
- Decreto 366/2017 del 21 de diciembre de 2017 reglamentó lo dispuesto por el artículo 244 y 245 de la Ley 19.535.

Autoridades Competentes

Se faculta al Poder Ejecutivo a adoptar las medidas preventivas y sancionatorias necesarias para evitar la proliferación de actividades de comercialización de juegos a través de internet, en especial el bloqueo de acceso a sitios web.

Solicitudes



*Juegos y apuestas deportivas por internet

URL afectadas	19	Solicitudes rechazadas	3

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

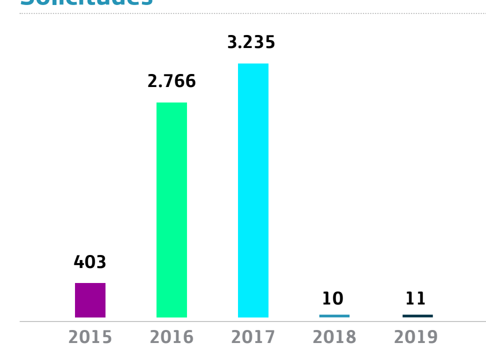
Contexto legal

Ley 19.355 (artículo 166): habilita al Ministerio del Interior a bloquear el ingreso de llamadas provenientes de servicios telefónicos al Servicio de Emergencia 911 cuando existan registros debidamente documentados que acrediten el uso irregular de las referidas comunicaciones en forma reiterada (más de tres comunicaciones en el mes o seis en el año).

Autoridades Competentes

Ministerio del Interior (Poder Ejecutivo)

Solicitudes*



*Suspensión temporal por un periodo de entre 3 y 6 meses.

Accesos afectados	1422	Solicitudes rechazadas	0







Venezuela

www.telefonica.com.ve

El Grupo Telefónica opera servicios de telefonía móvil en Venezuela desde el año 2005.

La Compañía tiene en Venezuela una oferta integral de servicios con productos en Internet móvil, televisión satelital y telefonía móvil y fija.

En 2019, los ingresos de Telefónica en Venezuela ascienden a 79 millones de euros y el OIBDA suma 19 millones de euros.

9.474
Accesos totales

Accesos a cierre de 2019 (datos en miles).



Accesos

344 Telefonía fija	**8.818** Telefonía móvil
6 Datos e Internet	**306** TV de pago

Accesos a cierre de 2019 (datos en miles).



INTERCEPTACIÓN LEGAL

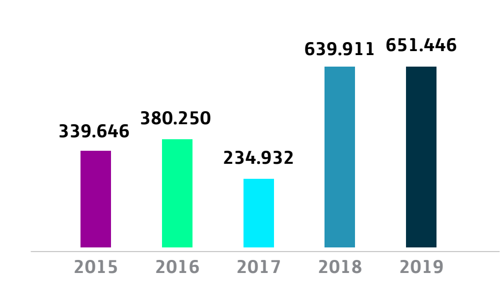
Contexto legal

- Código Orgánico Procesal Penal (Art. 205, 206).
- Decreto con Rango, Valor y Fuerza de Ley Orgánica del Servicio de Policía de Investigación, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas y el Servicio Nacional de Medicina y Ciencias Forenses (Art. 42).

Autoridades Competentes

- El Ministerio Publico a través de sus fiscales.
- Cuerpo de Investigaciones Científicas y Criminalísticas.
- El Servicio Bolivariano de Inteligencia Nacional (previa solicitud del Ministerio Público y autorización del juez correspondiente).
- Los cuerpos de policía debidamente habilitados para ejercer atribuciones en materia de investigación penal.
- Universidad Nacional Experimental de la Seguridad (UNES); demás órganos y entes especiales de investigación penal.

Solicitudes*



*No existen solicitudes de prorrogas y cese porque las únicas intervenciones que se realizan son solo las de ubicación y datos del suscriptor en tiempo real.

Accesos afectados	1.212.732	Solicitudes rechazadas	6.617

METADATOS ASOCIADOS A LAS COMUNICACIONES

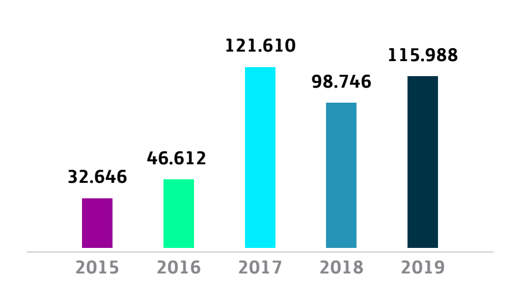
Contexto legal

- Providencia Administrativa N° 171. Normas relativas a la recopilación o captación de datos personales de los solicitantes de los servicios de telefonía móvil y telefonía fija a través de redes inalámbricas o número no geográfico con servicio de voz nómada.
- Ley contra el Secuestro y la Extorsión (Artículo 29).

Autoridades Competentes

- El Ministerio Público.
- El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC).
- Los componentes de la Fuerza Armada Nacional Bolivariana, dentro de los límites de su competencia.
- Autoridades de inteligencia policial.
- El Cuerpo de Policía Nacional dentro del límite de sus funciones auxiliares de investigación penal.
- Cualquier otro órgano auxiliar de investigación penal cuya intervención sea requerida por el Ministerio Público.

Solicitudes*



Accesos afectados	1.013.531	Solicitudes rechazadas	916



BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

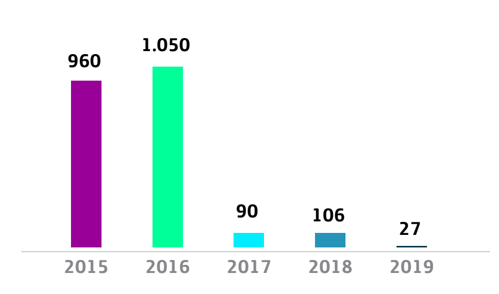
Contexto legal

- Ley Orgánica de Telecomunicaciones (Artículo 5).
- Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Artículo 27).

Autoridades Competentes

Comisión Nacional de Telecomunicaciones (CONATEL).

Solicitudes



URL afectadas	27
Solicitudes rechazadas	0

SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

La Ley Orgánica de Telecomunicaciones (Artículo 5).

Autoridades Competentes

- Ministerio de Transportes y Comunicaciones (MTC).
- Sistema de Defensa Nacional y Civil.

Solicitudes

2015	2016	2017	2018	2019
0	0	0	0	0

Accesos afectados	0
Solicitudes rechazadas	0



Glosario

CONCEPTO	EXPLICACIÓN
Autoridad competente	Jueces y Tribunales, Fuerzas y Cuerpos de Seguridad del Estado y demás administraciones u organismos gubernamentales a los que la ley faculta para realizar las peticiones objeto de este informe. Las Autoridades Competentes podrán variar en función del tipo de petición y de la legislación aplicable en cada uno de los países.
Datos personales	Se entiende por datos personales cualquier información que se refiera a alguna persona identificada o identificable, como puede ser su nombre, domicilio, destinatarios de sus comunicaciones, localización, contenido de las comunicaciones, datos de tráfico (días, hora, destinatarios de las comunicaciones, etc.).
Datos de localización	Los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de Red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada.
Datos de tráfico	Cualquier dato tratado a efectos de la conducción de una comunicación a través de una Red de comunicaciones electrónicas o a efectos de su facturación.
DPI	Son las siglas en inglés de *Deep Packet Inspection* o inspección profunda de paquetes. DPI identifica situaciones de falta de cumplimiento de protocolos técnicos, virus, *spam*, o invasiones, aunque también puede usar criterios predefinidos diferentes a los anotados para decidir sialgún paquete puede o no pasar, o requiere ser enrutado a un destino distinto, darle otra prioridad o asignación de ancho de banda, para tomar información con propósitos estadísticos o simplemente para eliminarlo.

CONCEPTO	EXPLICACIÓN
IMEI	Son las siglas en inglés de *International Mobile Station Equipment Identity* o identidad internacional del equipamiento móvil. Se trata de un número de serie que identifica al terminal físicamente. El IMEI le sirve al operador para identificar terminales válidos y que, por tanto, pueden conectarse a la Red.
IMSI	Son las siglas en inglés de *International Mobile Subscriber Identity* o identidad internacional de abonado móvil. Es el identificador de la línea o servicio. Este número sirve para enrutar las llamadas y se puede obtener el país o la Red a la que pertenece.
IOCCO	Son las siglas en Inglés de *Interception of Communications Commissioner's Office* en Reino Unido. Es responsable de mantener bajo revisión la interceptación de comunicaciones, la adquisición y divulgación de datos de comunicaciones por agencias de inteligencia, fuerzas policiales y otras autoridades públicas. Presentan informes semestrales al Primer Ministro con respecto a la ejecución de las funciones del Comisionado de Interceptación de Comunicaciones.
MAJOR EVENTS	Existen ciertas situaciones de fuerza mayor que pueden provocar las siguientes actuaciones: **1. Restricción o denegación del servicio**. (Incluyendo SMS, voz, correo electrónico, correo de voz, internet u otros servicios) que supone limitar la libertad de expresión. Ejemplos: > Restricción o denegación del servicio a nivel nacional. > Restricción o denegación de acceso a un sitio web(s) por motivos políticos (por ejemplo, páginas de Facebook; web de noticias –Ej. bbc.co.uk–; sitios web del partido de la oposición en el período previo a las elecciones; sitios web de grupos de derechos humanos, etc.).







CONCEPTO	EXPLICACIÓN
***MAJOR EVENTS* (cont.)**	> Desconexión específica de cualquier servicio de telecomunicaciones por motivos políticos. (Ej. en uno o un pequeño número de celdas). > Denegación de acceso a redes o a determinados servicios a ciertos clientes con el objetivo de limitar la libertad de expresión legítima de ese individuo. **2. Apagado de Red/control de acceso.** Ejemplos: > El cierre de toda la red a nivel nacional. > Control de acceso a la red en un área específica o en una región por motivos políticos. **3. La interceptación sin fundamento legal.** Situaciones en las que las autoridades interceptan comunicaciones sin tener una base legal por causas de fuerza mayor. **4. Comunicaciones impuestas por las autoridades.** Ejemplo: > Envío de mensajes/comunicaciones a nuestros clientes en nombre de un gobierno o agencia gubernamental por motivos políticos. **5. Cambios operacionales significativos.** Ejemplos: > Cambios, o propuestas de cambios, significativos operativos y técnicos respecto a los servicios de vigilancia (acceso a los datos, retención de datos e interceptación), que tienen como objetivo reducir el control por parte del operador para supervisar este tipo de actividades. (Ej. un cambio en el proceso para permitir el acceso directo por una agencia gubernamental/ gobierno). > Un cambio en el proceso para establecer vigilancia masiva. **6. Cambios legales significativos.** (Ej. cambios significativos –o propuestas de cambios– de leyes que dan a las autoridades gubernamentales más poder para hacer peticiones a los operadores). Ejemplo: > Cambios en las leyes de interceptación de comunicación.
PSI	El Portal de Servicio Interno "PSI" es una aplicación de consulta, permite que los integrantes de la Policía Nacional de Colombia, como clientes internos de la organización, encuentren en un sitio web toda la información para trámites internos, con altos niveles de seguridad.

CONCEPTO	EXPLICACIÓN
Solicitud	Una Petición es un requerimiento relacionado con la prestación de un servicio, en el ejercicio del deber de cooperación con las Autoridades Competentes. Una Petición puede contener una o varias solicitudes individualizadas, denominadas Solicitudes. Clases solicitudes: > Interceptaciones legales > Metadatos asociados a las comunicaciones: > Bloqueo y restricción de contenidos > Suspensiones geográficas o temporales de servicio
SUTEL	La SUTEL es un órgano de desconcentración máxima de Costa Rica, adscrito a la Autoridad Reguladora de los Servicios Públicos (Aresep); creada mediante la Ley 8.660, publicada el 13 de agosto de 2008. A la SUTEL le corresponde de la aplicación de la regulación al sector de telecomunicaciones y asegurar la eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura e información, así como mejores alternativas en la prestación de los servicios de telecomunicaciones.
TELCOR	El Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR) es el "Ente Regulador" de los Servicios de Telecomunicaciones y Servicios Postales, una institución estatal, la cual tiene como funciones la normación, regulación, planificación técnica, supervisión, aplicación y el control del cumplimiento de las Leyes y Normas que rigen la instalación, interconexión, operación y prestación de los Servicios de Telecomunicaciones y Servicios Postales.
URL	Son las siglas en inglés de *Uniform Resource Locator* (en español, localizador uniforme de recursos), que sirve para nombrar recursos en internet. Esta denominación tiene un formato estándar y su propósito es asignar una dirección única a cada uno de los recursos disponibles en internet, como por ejemplo páginas, imágenes, vídeos, etc.

